UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

UNITED STATES OF AMERICA,

v. 17 Cr. 548 (JMF)

JOSHUA ADAM SCHULTE,

Defendant.

Trial

----------x

New York, N.Y.
June 24, 2022
9:00 a.m.

Before:

HON. JESSE M. FURMAN,

District Judge
-and a Jury-

APPEARANCES

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
BY: DAVID W. DENTON JR.
MICHAEL D. LOCKARD
Assistant United States Attorneys

JOSHUA A. SCHULTE, Defendant *Pro Se*

SABRINA P. SHROFF
DEBORAH A. COLSON
Standby Attorneys for Defendant

Also Present: Charlotte Cooper, Paralegal Specialist

(Trial resumed; jury not present)

THE COURT: You may be seated.

All right. Welcome back. Good to see everyone.

We're resuming trial. Before we resume Mr. Leedom's testimony, anything to discuss this morning as opposed to at the break or at the end of the day?

MR. DENTON: Yes, your Honor.

At least from the government, we had a couple of issues related to proposed defense exhibits that we expect the defendant may try to introduce with Mr. Leedom that we wanted to raise. There are essentially three categories of proposed defense exhibits to which we have objection, at least one of which raises a separate concern.

First, we were provided yesterday by standby counsel with six articles from the internet relating to purported security vulnerabilities in various Atlassian products that were identified in 2021 and 2022. But aside from the timing of their production, we think there's an obvious hearsay problem, to say nothing of the 401 and 403 problems of arguments relating to vulnerabilities identified in different versions of software long after the events that are at issue in this trial. Those articles were not provided to us marked, so we don't have reference numbers for them.

There's a related set of materials that were provided to us, part last week and part on Tuesday, which were marked as

defense exhibits 1202, 1204, 1206, and 1207, which are reference materials, also apparently from the internet, which again, we think that to the extent the defendant wants to cross-examine Mr. Leedom about his conclusions, he certainly is entitled to do that, but he's not entitled to offer reference materials into evidence.

The third, however, and most sort of problematic category are the items that were marked as defense exhibits 1210 and 1211, which is code and then a compiled executable program of that code that appear to have been written by the defendant. That raises an evidentiary concern in the sense that those are essentially his own statements, which he's not entitled to offer but, separately, to us, raises a substantial security concern of how the defendant was able to, first, write but, more significantly, compile code into an executable program on his laptop.

You know, your Honor, we have accepted a continuing expansion of the defendant's use of a laptop that was originally provided for the purpose of reviewing discovery, but to us, this is really a bridge too far in terms of security concerns, particularly in light of the issues uncovered during the last issue with his laptop and the concerns that the MDC has raised to us about tampering with the law library computer. We have not taken any action in response to that, because we're in the middle of trial and we're loath to do things that would

disrupt the trial at this point. The fact that defendant is compiling executable code on his laptop raises a substantial concern for us separate from the evidentiary objections we have to its introduction.

THE COURT: OK. Maybe this is better addressed to Mr. Schulte, but I don't even understand what the third category would be offered for, how it would be offered, what it would be offered for.

MR. DENTON: As best we can tell, it is a program to change the time stamps on a file, which I suppose would be introduced to show that such a thing is possible. I don't know. We were only provided with it on Tuesday. Again, we think there are obvious issues with its admissibility separate and apart from its relevance, but like I said, for us, it also raises the security concern that we wanted to bring to the Court's attention.

THE COURT: OK. And with respect to the second category, the reference materials, I don't know what we're talking about there. Would it not fall within the scope of Rule 803(18)?

MR. DENTON: Your Honor, I think it is possible that they might. I think, on the other hand, to the extent that the defendant wishes to offer materials separate and apart from sort of cross-examination and through just kind of a generic, you know, introduction of them, there's some foundation that's

still required under the rule.

THE COURT: Right. Well, the rule, to be clear, doesn't actually allow the material to be admitted; it allows the statement to be read into evidence but not received as an exhibit. I don't know if that's the purpose of it. Obviously, it's still required to be marked, but it wouldn't come into evidence.

All right. Mr. Schulte.

MR. SCHULTE: Yeah. So, just starting with the first thing about the vulnerabilities, most of this stuff is very recent. We only -- it's from, some of this is from June, even. So we just discovered this. As soon as we obtained it, we provided it to the government. So the vulnerabilities, even though the versions of the software are newer now, the vulnerabilities date all the way back to very old versions of the software. So we think that it's relevant to the cross-examination to show the vulnerabilities in the software.

THE COURT: But is it your intention to offer the articles, because the articles are pretty much straight hearsay; no?

MR. SCHULTE: I mean they're not really articles in the traditional sense. They're security, security documents, some of which were produced through his company, we believe, MITRE. Or the MITRE company's involved with this -- so what it is is there's a tracking mechanism for vulnerabilities CVE, and

his company, MITRE, at some point was involved in this. So he -- the question is -- I don't know whether or not the document itself should come in. I think it's a technical document. It's not really a news article. It's about tracking of the vulnerabilities. So we think it should come in, but at the very least, we could show it.

THE COURT: That's not a distinction that is recognized in the hearsay rule. There's no exception for technical documents. It's an out-of-court statement. I don't see any reason why you can't ask the expert, are you aware that this tool has a security vulnerability and has always had it, if you can link it to the relevant time in this case, as opposed to some version of the software that postdates the events in this case by some number of years, which would be totally irrelevant. I think if you can link it and you can ask him directly, that's one thing.

What you can't do is either offer an exhibit that's an out-of-court statement by someone else or ask him, isn't it true that MITRE said X, Y and Z. Because that's also an out-of-court statement. In other words, you can ask him directly, but you can't ask about an out-of-court statement.

MR. SCHULTE: OK.

THE COURT: And I don't see a scenario in which these articles themselves come into evidence. Again, maybe if you say isn't it a fact that this Atlassian product had a security

vulnerability dating to whenever and he says I don't remember that, then you can try and refresh his recollection with it. But again, I don't see any scenario in which you can offer that article, let alone through this witness --

MR. SCHULTE: OK.

THE COURT: -- as opposed to the reference materials. Again, I would draw your attention to 803(18), which might permit you, if they would qualify under that rule, to have the witness read certain statements from it. But I don't see any scenario in which those out-of-court statements come in either.

MR. SCHULTE: OK. Understood. Yeah, I think just asking him about it, if he knows about it, in general, without bringing in the document, I think that's --

THE COURT: But asking if he knows about an out-of-court statement is asking about hearsay. So you can ask if he knows about the fact.

MR. SCHULTE: OK, yeah.

THE COURT: Not about the statement. Do you understand the distinction?

MR. SCHULTE: Yes, I do.

THE COURT: OK. And if he says no, I think you're basically stuck with that answer.

And then the third category, Mr. Schulte, the code situation, there are two separate issues there. One is the security issues, which I think are separate and apart from any

admissibility issues, and we can take up separately if or when there's an application on that front.

MR. SCHULTE: Yeah, and we can circle back to the manuals. But for the code, the government produced lots of source code in discovery, and this specific file is, like, ten, ten lines of source code as well as --

THE COURT: Where does it come from? Did you write it?

MR. SCHULTE: Yes, I wrote it. That's correct.

THE COURT: How do you intend to offer that? It is a statement of your own.

MR. SCHULTE: Well, so, like I -- so, it may -- it may help to go back to the manuals. So, there are several technical manuals that he should be aware of in some technical library. So based on that, what I intended to do was show him those documents from Microsoft and other providers that -- he should know this information, and from that I would then show him the seven lines of code, ask him if he recognized -- it's basically the same thing from the library, just tweaked to specifically show an April 20 modification and basically ask him if he knows, understands and knows what this is. It's no different as if he wrote it or some other, random person wrote it.

The point is the functionality and what the code can do and how quickly it is to write something like that. I think

that's the point of the testimony, to get out how easy this is to do. It doesn't take -- anyone can do this easily. It's on the internet for how to do this. It's proper, like, expert cross on that information. And then, this, I don't know from there, then to have him, once he explains exactly what it does or how it works, to potentially just -- it's just a double-click this thing, the program, and then it just shows how the file time is changed. So that, I think, is separate. It's almost a demonstrative of how the source code works. But I think the source code is proper for the expert to be able to explain how it works, how easy it is to do. And I think the demonstrative of the executable is a separate thing. But I think would go -- it's just a guide to show how that works and how it would show up in Windows and how the file times get changed.

THE COURT: All right. I think what we're going to have to do is take it up as it comes, see what Mr. Schulte tries to do with it, mindful of the limitations on what he can and cannot offer. I'm not sure the code, depending on how he uses it, it may not be offered for the truth *per se*, in which case I'm not sure there's a hearsay problem. But we'll take it as it comes, I guess.

MR. DENTON: Your Honor, I think there's two issues.

The first is it seems like his purpose is to offer it for the truth that these statements that the defendant wrote do

this thing that the defendant asserts they do. So I think that does -- I mean we're in a little bit of a strange posture here.

The second issue that we have is, again, this is something that was only provided to us on Tuesday morning. We didn't have a chance to review it until Mr. Leedom was already on cross. We only had a limited ability to see what it is and figure out what it is, and that's been bound up in these security issues. There's no reason this is something that should be coming at this point, and so we think there's a separate issue there as well.

THE COURT: All right. But Mr. Denton, Mr. Schulte could theoretically put a white board up and say, Mr. Leedom, isn't it the fact that I could write a line of code that says this and I could write a line of code that says this, and it would result in the log files being deleted in this way, or whatever, assuming that there's a relevant conclusion there. Right? I'm not sure it's different than that except that it was provided in advance. Again, I don't know if it's going to come in. I think we have to wait and see what he tries to do with it, and I'll take up any objections at that time. I appreciate the heads-up, but I think we'll have to wait.

MR. DENTON: That's fine, your Honor, but I think even doing that would raise serious issues about the defendant essentially testifying in that way by putting these things, you know, statements that -- code occupies sort of a weird

category. Obviously, it's a little bit different, but I think there's still an issue there.

THE COURT: And do you have any law for the proposition that code is, if offered to show that code can produce a particular result -- in other words, that it results in a computer doing something -- that that's a statement offered for its truth? Because it seems to me that's more in the nature of a command, and that obviously wouldn't be hearsay.

MR. DENTON: So, I think admittedly, your Honor, there is not law on this particular issue. I'm not aware of anything that sort of presents this kind of analogy.

Again, we recognize that what the Court wants to do is take it as it comes, so we'll be prepared to do that.

THE COURT: All right. And what are the reference materials? What were those exhibit numbers again?

MR. DENTON: 1202, 1204, 1206, and 1207, which, I think it's a little bit difficult to put them in the 803(18) category because they are essentially sort of user guides published or, you know, promotional materials published by various companies for these products. Again, we're happy to take it as it comes based on Mr. Schulte's cross-examination. It's obviously fine for that to inform his cross-examination and to ask questions premised on it. Our principal objection is to the introduction of the materials.

THE COURT: Again, I don't see how they would be admitted as exhibits themselves, but depending on the foundation that's laid, he may be able to elicit things that are in it from Mr. Leedom under the rule.

All right. Anything else that we have to take up now?

There are a couple of matters the government raised in two classified submissions yesterday that I think we should discuss in closed session this afternoon as opposed to here, although, Mr. Schulte, to the extent that one of them pertains to issues that may come up on cross, I would urge you to be careful and mindful of what the government has said in that letter. But anything that we need to discuss this morning?

MR. DENTON: Not now, your Honor. Thank you.

THE COURT: Mr. Schulte, can we get the witness and the jury?

MR. SCHULTE: I mean I think there's a, an issue here because some of my cross pertains to one of those issues that the government is kind of raising for the first time. They've been public. There have been public filings on this. I mean I don't know if the government's saying that the acronym's classified.

It puts me in a difficult position because I have, maybe, several cross questions based on this that I don't think is classified, has never been alerted to be classified. It's in public filings. So I was just talking to them before. I'm

not sure what they're trying to say is classified. So I don't know if there's some way to quickly just clear this up.

THE COURT: Mr. Denton, mindful that we're in open session, I don't know what we can --

MR. DENTON: The acronym, AFD, has been declassified. The substance of work related to that or other details of it remains classified and has only been produced in classified discovery. We've been careful about what has been said in the public filings. We don't think it's crossed that line, mostly because it's been demands by the defendant for documents which the government understands do not exist, so there hasn't been a need to engage on that substance in any public filings. But the substance of the material has always been marked and provided as classified.

THE COURT: OK. That's certainly consistent with my impression.

Mr. Schulte.

MR. SCHULTE: I think my questions would just be kind of consistent with some of the questions I've asked before, basically relating to the expert's work with AFD and, you know, if he's aware of some of the reports and findings that the AFD has, has had.

THE COURT: OK. Well I think --

MR. SCHULTE: That's OK, right? Or --

THE COURT: Well, to the extent you're citing a third

party's out-of-court statement, there's a hearsay issue --

MR. SCHULTE: Right.

THE COURT: -- separate and apart from the classified issue, so that doesn't seem OK to me. And I'm not sure what relevance crossing this witness about his knowledge of an office that may or may not, what that office does when it doesn't pertain to his investigation would have.

MR. SCHULTE: Right. So, no. He specifically worked with them, so just the question would be were you able to, through your work with this, with AFD, did you, were these the conclusions you reached? So it's specifically through his forensic examination and his forensic work with AFD, they reached certain conclusions, technical conclusions together.

THE COURT: OK. Well, I think there's another question asking this witness about the technical conclusions that he reached, but I don't see why that requires delving into what AFD does or is or what conclusions it may or may not have reached, again, much of which would be hearsay in any event. I urge you to be careful. It doesn't sound like anything you want to ask him would necessitate getting into the particulars of what AFD does, let alone any conclusions he's drawn, and you can certainly ask him directly about conclusions that he has drawn. But I think we'll leave it there for now.

MR. SCHULTE: OK, yeah.

THE COURT: All right. Let's get Mr. Leedom and the

jury, please.

(Continued on next page)

(In open court)

PATRICK THOMAS LEEDOM, resumed.

(Jury present)

THE COURT: You may be seated.

Good morning, ladies and gentlemen. Welcome back. Thank you for being here on time this morning. Sorry we're getting off to a slightly later start than I would like, but I appreciate your being here. I hope you had a nice midweek break and got back to your regular lives for a couple days.

We'll pick up where we left off, with cross-examination of Mr. Leedom.

Mr. Leedom, I remind you that you remain under oath. I'll also ask you at this time to remove your mask and also just remind you to speak loudly, slowly, clearly, and into the microphone.

THE WITNESS: Yes, sir.

THE COURT: With that, Mr. Schulte, you may proceed.

CROSS-EXAMINATION CONTINUED

BY MR. SCHULTE:

Q. Good morning.

A. Good morning.

Q. I'll start with admitted Government Exhibit 1207-36. Exhibit 1207-36 shows the contents of the Altabackup directory, correct?

A. Correct.

Q. This is where the backups are stored, correct?
A. That's correct.
Q. Now, you testified on direct about a snapshot and a reversion, correct?
A. Correct.
Q. For the purposes of the next few questions, I'm going to refer to this as the snapshot reversion theory. OK?
A. OK.
Q. And it's fair to say that the thrust of your testimony on this issue rested on the premise that there were strict access controls to this directory and its data, correct?
A. A piece of it, yes.
Q. I mean that's the whole purpose of it, isn't it?
A. Of accessing, of whether or not you accessed it using the virtual machine, because that's the only place it could be mounted?
Q. That was your testimony, right?
A. Correct.
Q. And it's your working hypothesis that the Altabackup directory could not be accessed because of strict access controls, correct?
A. That's correct.
Q. And because one could not access Altabackup, one needed to resort to taking a snapshot and undertaking a reversion, correct?

A. That's one method, yes.
Q. And it's fair to say that if one could access the directory shown in 1207-36, then a snapshot reversion is irrelevant, correct?
A. Yes.
Q. OK. So the safest way to determine access controls is through forensic analysis, correct?
A. It's one method, yes.
Q. Well, that's the easiest or safest way to do it?
A. I mean you could review the, like, the permissions on the folder. I guess you could call that forensic analysis, yes.
Q. Viewing a folder, yeah, but the CIA gave you full access to everything on DevLAN. Correct?
A. Correct.
Q. And in fact, you listed access controls for other directories on that Altabackup server, correct?
A. That's correct.
MR. SCHULTE: I'm going to show what's admitted as 1207-49.
Q. So this shows several of the directories on the Altabackup server, correct?
A. Correct.
Let me take that back. It's on the file share. It's not the Altabackup share. The shares are very distinct and different.

Q. It's on the same server?
A. The same file server, yes, that NetApp file server.
Q. OK. And now, 1207-50 is the properties tab of one of those folders, the source code and binary Gold copies, correct?
A. Correct.
Q. OK. And admitted 1207-52, this shows access controls, right?
A. It does.
Q. We've talked a lot about access controls, and this is just a great way to show what that means, what we've been talking about, right?
A. Yes.
Q. And these are access controls specifically for this directory source code and binary Gold copies, right?
A. Yes, that's correct.
Q. We have different -- we can see the types in this column, right? This is an allow list, right?
A. Yes.
Q. The group or the individual users listed under the principal column, right?
A. Yes, that's correct.
Q. And then the access is here. So we have several different types: Read access, so someone can actually look at the documents, right?
A. Yes.

Q. Read and execute, and full control, and that encompasses everything. You can write to the folder, you can edit the documents, everything, right?

A. Correct.

Q. OK. Inheritance and then what it applies to, other subdirectories and the files and basically how the allow-access control applies, correct?

A. Yes, that's correct.

Q. So if you run the same tests on the Altabackup directory, what permissions are listed?

A. Well, you can't really run the test the same way.

Q. And why is that? You can't pull this up on the Altabackup directory like this?

A. Well, you could in the environment that this was being, like, reviewed in, but it was shared differently. The share for Altabackups was an NFS share, which is very different than the type of protocol used to share the folder that we're looking at right now, and, like, the home folder and other folders. It's very different. The way permissioning works, it's very different.

Q. OK. But you can still pull up access controls such as this for shares like that, right?

A. That share wouldn't be able to be, like, mounted in this way. You can -- you can, like, pull up access to it and I think it would probably just say, like, you just have to be

root to access it, but you would have to be on the allow list for the actual server to be able to mount it in the first place. It's just -- it's very different. It's not a, like, a Windows share, so the permissions and things like that are different.

Q. So I'm asking, though, the access controls for that directory, no, I understand it's not the same as this, but just similar, you can have similar types of access controls. And what were those access controls on the Altabackup directory?

A. So, from what I understand, from the, like, when we got there and the available configuration of that file server, you know, a year later, when we got there, the Altabackup share was just, like, I think you just had to be, like, root to access it. But from everything else we've reviewed, not only do you have to be root, but you have to be root and you have to be on the allow list. Like, your computer would have to be in that allow list for IPs, which is pretty standard for how NFS servers are usually set up.

Q. I'm just asking specifically during this type, April 2016, what were the access controls? Do you have a document that shows what the access controls were for that directory?

A. Altabackup in 2016?

Q. Yes.

A. No, no. You have to talk to, I guess, ISB. They were managing it at the time. But there's no, like, historical

audit for the NetApp for -- for that.
Q. So you have no -- you have no ability to testify about what access controls existed on this directory in 2016, is that correct?
A. No, because we can use things -- like, when you attempted to mount it on the ESXi server and we saw that that failed, that shows that there was access control enabled on that share.
Q. We'll go into the data store in a little bit, but essentially, you're not relying on any document or any technical access control list; you're just inferring from what you've reviewed, is that correct?
A. Right. You got to look at everything as a whole.
MR. SCHULTE: OK. Let's take a look at the data store. I think this is slide 58 in your presentation.
Q. This is what you're referring to, right?
A. That's correct.
Q. And the data store is essentially just the way it sounds, a storage space for data, right?
A. It's -- yeah, it's like an object that you can use to access data, whether it's on the server itself or in a remote location; in this case, a remote location.
Q. And it basically just gives you a new folder to store data?
A. Essentially, yes.
Q. OK. Creating a data store is a typical administrative function, right?

A. Yeah, it's something you would do to manage the -- manage the server.

Q. And in fact, the Altabackup data store previously existed on the ESXi server, correct?

A. I don't believe so.

Q. Did you review the forensic logs about the data stores on ESXi?

A. I did.

Q. And did you see that there was a data store for Altabackups previously mounted?

A. The only data store Altabackups that I remember seeing is this exhibit here, 1209-7.

Q. This is the only thing you've seen about the Altabackups?

A. This is the only thing I've seen about an Altabackup data store --

Q. OK.

A. -- on ESXi.

Q. Regardless, the failure here to create the Altabackup data store does not necessarily tell you anything about the access controls on Altabackup, correct?

A. Oh, I disagree.

Q. You disagree with that?

A. Yes.

MR. SCHULTE: All right. Well, let's go back to slide 57, right before here.

Q. So here, you testified on direct that I log in as a regular user, correct?
A. That's correct.
Q. OK. Using my own credentials, correct?
A. Yes.
Q. And you testified on direct that this regular user account is not an administrative account, correct?
A. From what I understand, yes.
Q. So the failure to create the data store could and most likely occurred because a regular user simply does not have access to perform the mount, correct?
A. Well, the type of error that we received -- if you go back to the other --
Q. Well, no. I'm just asking based on this. If you're a regular user, you're not going to have the ability to be creating and mounting directories, right?
A. I'm not sure exactly, because there -- I don't think I had, like, audit for the user individually, like, at that level on that server. So I don't know if there's, like, a, you know, an explicit permission for data store management or not. But from the type of error that is shown, it leads me to believe that's more of a -- the NFS server actually denied the request and not the ESXi server saying you don't have the correct permission to, you know, create a data store. It was a -- the NFS server itself said I'm not going to let you do this, if that makes

sense.
Q. Well, I mean error messages can be misleading, correct?
A. Sometimes. I think in this case it's pretty clear.
Q. I mean you just -- your testimony is -- you're just speculating based upon a single error message here and a single failure, correct?
A. I mean it says it was denied by the NFS server. It doesn't say it was -- like, it doesn't say something like you don't have permission to create a data store. That's how I'm drawing my conclusion.
Q. But it also doesn't say that -- it doesn't say anything about what or how much access controls the NFS server even has, right?
A. No. That wouldn't be in an error message.
Q. You're also aware that OSB had its own subnet, correct?
A. Just from, like, a networking perspective. I don't know -- I'd have to refer to, like, the network documentation.
Q. Well, here, we can look at slide 52, and we're showing -- this is the IP address, 10.3.2.35, correct?
A. Correct.
Q. And this is on the 10.3.2.1 network, correct?
A. That's correct.
Q. OK. And we know the Altabackup is on a different network; it's on the 10.3.1 network, correct?
A. I believe -- I think I just remembered it ended in like,

dot-70, I think.

Q. You don't remember it being --

A. Yeah, 10.3.1.70.

Q. Yeah. That's a different network, right?

A. It's a different subnet. I mean they're obviously connected. To the extent of, like, which IP ranges or in which subnet and how they're connected, I can't really speak to.

Q. The failure here could simply be that this is on essentially a different network, correct?

A. I mean we know that the other servers had access to it. I mean without network logs, can't really speak to that. Obviously, the ESXi server was able to speak to the NFS server, because the log says the NFS server denied it. So that connection is definitely being made here. So I wouldn't say it's being blocked by some kind of firewall or something on a different subnet, but --

Q. OK. But the configuration for the NFS could simply be not to share with this subnet or to only share within its own subnet, right?

A. Could be. That's kind of how, one way you could set up the allow list. You can say block a whole subnet. You can say only allow certain IPs.

Q. And if it was set up that way, every other user, or most everyone else who's on the same regular network would then have access to the Altabackup directories, correct?

A. No, that's not how -- that's not how it works.
Q. That's not how what works?
A. If you have a explicit allow list -- I mean you can have both. You can have a deny this entire subnet and only allow, like, certain machines from another subnet. There's no reason you can't have both.
Q. Yes, but it could be configured just to deny from the OSB subnet; it could be configured to allow from the regular network, 10.3.1, correct?
A. I guess the only, like, real conclusion I want to draw from those permissions is it seems to me from my review that the most likely setup for that share was that it was allow-listed explicitly for the servers that needed to back up to it.
Q. What is that based on, though?
A. Well --
Q. What forensic evidence or what evidence do you have to base that conclusion on?
A. Well, both speaking to the admins themselves from ISB as well as their log like this. I mean it's -- put that together, it's very telling.
Q. Speaking with the admins, you're talking Dave, Dave C., right; he was one of those?
A. Yeah, Dave.
Q. And he was an employee who put the Stash on a hard drive, correct?

A. I know I've heard some of that. I don't know exactly the situation around that, but --

Q. But that, basically this hard drive with Stash was lost, correct?

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Well, to this day, no one knows where that hard drive is, right?

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. DENTON:

Q. OK. Dave C. is the one who set up the Altabackup share, correct?

A. I don't know if he's the one who, like, first set it up. I know that he worked on, like, the infrastructure and managed it. I don't know actually who set it up initially.

Q. Well, Dave C. set up the Altabackups without any access controls, right?

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. You would agree that the access controls to Altabackup are critical, right?

A. Yes.

Q. As part of your investigation, you spoke to Dave C., right?
A. I don't think I spoke to him, like, directly, like, face to face.
Q. So for the access control, greater access control means fewer people would have access to the data, correct?
A. I'm sorry. Could you say that again?
Q. Greater access control or more refined or more access controls typically means fewer people have access to the data, right?
A. That's correct, in general.
Q. And the opposite is true also -- if there's none or very limited access controls the access is less controlled, right?
A. On principle, yes. I think there's something else to unpack there, but yes.
Q. So what -- based on your forensic analysis, what evidence did you find or what forensic evidence did you find to suggest that there were more refined or more restricted access controls rather than very basic, limited access controls, like limiting OSB subnet?
A. Just for Altabackup?
Q. Yes.
A. I mean we're looking at the main piece of evidence that I have that, you know, that we have that kind of supports that, is the -- we can see that the data store failed to mount, and there was a message from the NFS server that said there was a

failure.

Q. Right. But the point is that message would occur if only the OSB subnet was denied. If the only access controls in Altabackup was deny OSB or deny to any subnet besides the network it's on, you would see this message, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Let's move on, Mr. Schulte.

BY MR. SCHULTE:

Q. OK. Just to be clear, for the access controls here, you have no documentation or no configuration files showing the exact access controls, right?

A. We do not have a configuration file for Altabackup from the NetApp that, like, shows the -- the allow or block list. It just wasn't available at the time.

Q. All right. And on that same point, as part of your investigation, you were not able to conclude absolutely, forensically, that there were strict access controls on the Altabackup directory, correct?

A. I disagree. Just --

Q. I mean you're just basing it off this one finding, but you don't --

A. This finding and knowledge of the network and what I've heard from the admins on the network.

Q. What you've heard from the admins, though, I mean --

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. What you heard from the admins is not forensic, correct? I'm just talking about forensics.

A. It's not, like, an artifact on the network, but --

Q. There's no artifact on the network that says that these were access controls, and you are just speculating as to what the access controls are, correct?

MR. DENTON: Objection to form.

THE COURT: Sustained as to form.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. There are no forensic artifacts, correct, that specifically restrict the access controls to the directory? Right? Again, you're just -- let me just be clear. You're just -- based on this one piece of evidence, you're speculating and that you could be wrong, correct?

MR. DENTON: Objection to form.

THE COURT: Sustained as to form.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. OK. The only forensic artifacts -- there's no forensic artifacts about the specific access controls; however --

THE COURT: Let's start that one over. Sustained as to form again.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. So your conclusion is only one of inference, correct?

A. Aside from --

Q. You're inferring based on this, right?

A. Based on this exhibit and the other stuff I mentioned, yes.

Q. What stuff, sir?

A. The, like, the testimony from Dave.

Q. Those aren't forensics. I'm talking about forensics, sir. What forensics do you have besides this?

A. Besides this, I started to say before, we don't have a, like, allow list configuration from the NetApp, like I'd mentioned previously.

Q. OK. So you're just inferring based on this, and that could be wrong, right?

A. I don't think it's wrong.

Q. It could be wrong, right; you don't know?

MR. DENTON: Objection.

THE COURT: Sustained.

Let's move on, Mr. Schulte.

MR. SCHULTE: All right. Let's turn to slide 113.

Q. Now, your presentation here leaves out a couple of major events at the beginning, does it not?

A. I think you're going to have to elaborate.

Q. You didn't put on your slide that after the command listing

files, at 5:29 p.m., the very next command there's a listing of files --

MR. DENTON: Objection.

THE COURT: Let Mr. Schulte finish the question, please.

BY MR. SCHULTE:

Q. -- at 5:55?

A. Can you repeat the question? I'm sorry.

Q. Yeah. So, you didn't put on your slide or you didn't show that after the command listing files at 5:29 p.m., that the very next command is at 5:55 p.m., correct?

A. I'd have to look at the -- like, there is a lot of activity, so what we kind of cut down for the PowerPoint summarizes the, like, the main points.

Q. All right.

A. If you have, like, like a list command at 5:29 and want me to look at it, I'd be happy to look at it, but --

THE COURT: Mr. Leedom, just a reminder to slow down. Keep your voice up. Don't swallow your words. Speak, loudly, clearly.

THE WITNESS: Yes, sir.

MR. SCHULTE: I'm just going to show the witness and the parties something marked defense exhibit 1209.

Q. Now, do you recognize what type of file or what this shows? Do you recognize it?

A. Yes.

Q. And it's, you know, it's one of the other types of files that you've exhibited throughout your presentation, right?

A. Yes.

MR. SCHULTE: I move to introduce defense exhibit 1209 into evidence.

MR. DENTON: No objection.

THE COURT: Admitted.

(Defendant's Exhibit 1209 received in evidence)

BY MR. SCHULTE:

Q. And this is a transcript file showing remote access to the ESXi server, correct?

A. This is -- I believe this was recovered from unallocated space on your virt. machine.

Q. It's from the CIA workstation, but it's showing remote access on the ESXi server, right?

A. That's correct.

Q. And it's recording the commands as they're being typed from the workstation, correct?

A. Yes.

Q. OK. The first command executed here is LS-ALTR, correct; it lists the files?

A. That's correct.

Q. And this is the, you're basing it off the shell log, and it's showing it's 5:29, correct?

A. Yes. If this is the end of the, of the previous command, then yes, that's how I would have time stamped that.

Q. This is right at the beginning of your time line, right?

A. At 5:29? Yes.

Q. Yeah.

All right. And the very next command is another LS-ALTR, right?

A. Yes, it is.

Q. And this command is 5:55 p.m., correct?

A. Yes, it appears to be.

Q. And this is after the backups are supposedly accessed, right?

A. I believe so.

Q. So between this command at 5:29 and the very next command at 5:55, there are no commands here, right?

A. Not in this exhibit, no.

Q. I mean this is recovered directly from the workstation, right?

A. Yeah, from the unallocated space. Yes.

Q. OK. But if there were commands -- well, specifically, there's no command SSH into the Confluence machine, right?

A. No. We don't have it here in this exhibit. I'm not sure if it would be in this regardless for that. But I mean, no, there's no SSH command here.

Q. I mean if the SSH command here was run here, you would see

it, would you not?
A. I'm not sure how exactly, like, how this, like, you called it a transcript, like, how it was, how it came to be. So we got it from deleted space, so --
Q. I think we'll go into detail about the transcript file a little bit later, but the point is this is -- you're seeing the output of all, of all the commands that are being executed, correct?
A. That's correct.
Q. If this, if there was a log-in, or if there was a log-in and commands were being executed on the Confluence system, we would see that here, right?
A. We have commands from the OSB server. We don't have commands, like, from the Con -- like, the Ubuntu VM itself.
Q. Well, there's no difference between this OSB server and Confluence server; they're both servers, right?
A. Well, but this is from a single, like, SSH session.
Q. OK. And I mean you -- you show in your presentation, you know, all these events that are occurring during this time frame, right?
A. Yes.
Q. OK. And specifically, there's no command here to SSH into the Confluence very many, right?
A. There's no SSH command from the ESXi server into the Confluence VM.

Q. There's no SCP command either, right?
A. Not from this log from the ESXi server.
Q. Well, this is from the CIA workstation. It's from my workstation, right?
A. It is, but it's from a session from the ESXi server.
Q. Showing a remote session into the ESXi server, right?
A. Yes.
Q. But it doesn't show any SCP command, right?
A. No.
Q. And that's the secure copy; that would be what you would run to copy something from the server, right?
A. That's a command you could use to do that.
Q. OK. There's no other copy command that you would run -- there's no other copy command either here, right?
A. No, there's not.
Q. OK. In fact, there's no trace of any log-in to the Confluence VM during that reversion period, right?
A. Not in this, in this exhibit, this log, no.
Q. Well, not just this exhibit; all the, all the, all the transcript files that you reviewed, right?
A. Yeah, all the connections from the OSB server, there's -- there's, like I said, there's no, like, SSH from the OSB server to the Confluence server.
Q. Well, there's also transcripts from the actual workstation itself, right? The workstation, you have to run a command to

access the ESXi server, correct?
A. Yes, you do.
Q. OK. And you testified on direct that these commands don't exist because the Confluence virtual machine was reverted and deleted, right?
A. So that's running from the inference that there's --
Q. I'm just asking if that's your -- that was your testimony, right?
A. Yeah, that's why we don't see, like, a copy command.
Q. But of course, reverting or deleting the Confluence virtual machine has absolutely no effect on transcript files from my own CIA workstation, correct?
A. That's correct. If we're calling those -- the exhibits of all the commands, if that's what we're calling transcript files, we can call them that.
Q. OK.
A. I can't determine, you know, exactly what their source is there, but --
Q. We'll get into that later, but -- so your testimony then from direct is not correct, right? Your testimony that you said you don't, these commands don't exist because the Confluence virtual machine was reverted and deleted, that testimony is wrong, right?
A. No.
Q. You just said, you disagreed that reverting or deleting the

Confluence virtual machine has no effect on the transcript files from my own CIA workstation, right?

A. Assuming that -- figuring, that there is transcript file for that activity in the first place. What I testified to on direct was that there's no copy command -- in my opinion, the copy command would be in that Confluence virtual machine, should be on the virtual machine there, and that's where you'd be running, running those commands from.

Q. I mean, you don't have to -- you could run the commands from anywhere; you don't have to log in to the Confluence machine to run the copy command, right?

A. You could use SCP, which you would have to -- I mean that does have to log in to the machine to do that.

Q. Right.

A. So the logs of that log-in would be on the VM, which were deleted. That's what I'm testifying to, is that any activity that would have affected files connected to that Confluence virtual machine was deleted. So, you know, that could be a copy command. That could be an SCP session to copy to the network that's authenticating, things like that.

(Continued on next page)

BY MR. SCHULTE:

Q. So your testimony is the logs on Confluence are no longer available, right?

A. That's correct.

Q. But any transcript file or any log from my work station would still be available, right?

A. I wouldn't say any. I don't know these circumstances around what makes the transcripts when they're there, what turned them on and off, things like that, but all I can really speak to is the evidence that's here about all the activity on the ESXi server itself and I think, like you said, there is some from the -- from the VM itself.

Q. I mean, if we look at this, you know, this was -- if this was a server, a virtual server and it was reverted, these files would remain on my work station, right?

A. Yes, because it came from your virtual machine.

Q. So the point is anything that you do to another server or another system is not going to affect logs or documents being produced on this work station, right?

A. That's correct.

Q. OK. Essentially since the source of these transcript files is my CIA work station, they are preserved no matter any snapshot or reversion, right?

A. Correct.

Q. And if I logged in here, or if I ran an SCP command here,

you would see the transcript files on the CIA work station just like you do the ESXi server, right?

A. I mean, I can only speak to what we recovered so we didn't recover any commands like that.

Q. So I think your testimony though, on direct, was that these commands would not be here at all, correct?

A. Like I said before, my testimony is about the actual Confluence, like virtual machine itself, and those logs which were deleted from the snapshot reversion, not that there, you know, could be commands in a transcript that was missing and not being able to be recovered from your work station.

Q. OK. So your testimony is specifically just about any logs that were on Confluence, right?

A. Yes, specifically to, like, copy command, that kind of thing; yes, that is correct.

Q. But as for the transcript files, unallocated space, and my work station, you looked everywhere there for a copy command during the reversion; correct?

A. Yes. I searched through it for alt commands, not just copy, but.

Q. You were really looking for copy commands, right?

A. I mean, sure. Copy commands, like I said, any commands are really valuable so it is not like I searched only for copy commands.

Q. You really scrutinized the work station over the last five

years, right?

A. Not like every day over the last five years but, yes, it was reviewed in some time in the last five years.

Q. You did a complete forensic analysis on the work station, right?

A. That's correct.

Q. You looked for a copy command during the reversion period, right?

A. Yes.

Q. Looked high and low, right?

A. That's correct.

Q. You did not find a copy command during the reversion, correct?

A. No.

Q. You did not find any logins to the Confluence virtual machine during the reversion, correct?

A. No, not that I believe.

Q. And you know all these very specific times on your timeline from the transcript files, right?

A. There are still estimates, I would call them very specific estimates, but yes.

Q. I mean, the point is there is no -- there is no files that were deleted or activity that was executed that is not -- that you didn't find transcript files for, right?

A. Included in the timeline here as far as everything on the

bottom? Everything on the bottom here comes from transcript files aside from the vault stuff.

Q. If you hire a painter to paint a room, how many times do you have to check the room to know he didn't paint it yet?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. OK. Once and for all, forensically, based upon only your forensic findings, can you say that I copied the March 3rd, 2016 Confluence backup on April 20th, 2016?

A. There is no copy command, like, attributable to you for that.

Q. Just the forensics, based on your forensic findings?

A. I think taking them all together is part of the finding but there is no, like -- we don't have a forensic artifact of a copy command for that.

Q. Back to the logs. You have all -- again, you have all the logs from the CIA work station, right? From my CIA work station?

A. That we were able to recover, yes.

Q. You testified they're all in tact, right? There were no deletions of those files, right?

A. Yes. On the host I don't recall seeing like any evidence of deletion.

Q. And this includes logs of removable media, correct?

A. Yes.

Q. You have the logs for every device I ever connected into the CIA work station for how long, right?
A. Yes, in a general sense.
Q. And you also recovered every single device I connected into the CIA work station, right?
A. I don't remember from, like, an inventory perspective. I don't remember.
Q. During the reversion period there are no removable media connected to my CIA work station, correct?
A. I don't believe so. I don't think there was artifact of that. I know there was one that was connected, like, recently, the one that was connected to a write blocker, but I think that was -- that might have been on the 18th. Maybe. I don't quite remember the date for that but no to my knowledge I don't believe there was a USB artifact from during the reversion period from your work station.
Q. If there had been one you would have put it in your presentation, right?
A. Yes.
Q. It would have been important that removal media or large hard drive was being plugged in, right?
A. Yes. That would be important.
Q. And there are no forensic artifacts showing any of the Atlassian backups copied to my CIA work station, right?
A. No.

Q. In fact, the virtual machine was only 50 gigabytes, right?
A. I don't remember the exact size.
Q. You don't remember the exact size?
A. No.
Q. But in any case, there is no -- you have the unallocated space and you have all the forensic artifacts that you are able to find like link files and open files, all this forensic evidence that you went through and there was no evidence of any backups on the computer, right?
A. No, not on your work station.
Q. There are no forensic artifacts showing any of the Atlassian backups were ever copied to any devices I possessed or used at the CIA, correct?
A. Not to my knowledge.
Q. In fact, you never even suggest through your whole 150-slide show, you never present a theory for a copy, correct?
A. I think I did present the theory for the copy in that it happened during the reversion period on the Confluence virtual machine, but.
Q. I mean, without any removal media connected to my CIA work station during the reversion it is not possible to steal the backups, is it?
A. I mean, there is attached network shares, there is other ways than just removal media. You could stage the data or move it.

Q. I mean, you found no evidence of any of that though, right?
A. I don't have a whole lot of visibility for some of that.
THE COURT: Can you explain what you mean by attached network share?
THE WITNESS: Yes. So like we saw, as an example, like the home folders, that's all connected over the network to the various work stations so, like, that could be a potential location something could be copied to. It doesn't necessarily have to be copied straight to the machine.
MR. SCHULTE: Object.
BY MR. SCHULTE:
Q. All right. The point is, though, your review of -- you had the whole DevLAN network and on your review of all these systems you didn't find copies to those, right?
A. Not to my -- not that I remember, like a -- but -- go ahead.
Q. You would have, from the CIA work station if there was mounted directories or mounted network shares, you would have seen logs of those; right?
A. I think most work stations had, like, home folder, those basic shares that we looked at mounted already so it is not like you have to make a new mount, but.
Q. So what exactly is the working theory of how this data was copied?
A. That it was copied during the reversion period from the

Confluence VM.

Q. But again, you said there is no forensic artifacts of those copies, right?

A. No, because you deleted all of the locations where --

Q. Again, you are talking about the Confluence system. There is no deletions from my -- from my logs, right?

A. I mean, from what we were able -- there is no -- what do you call it -- like copy commands from your virtual machine from what we recovered, no.

Q. OK. So -- and again, with no removable devices connected, no logs that you have shown of network shares or copies to network shares -- I am struggling to see what would have the Confluence backups have been copied to?

A. So like I said, it could have been copied to a network location. I mean, it's tough in general because when we arrived on site it was a year afterwards and, like, we have spoken to the availability of network logs and some of those things are just not available. So, like, from all the evidence retrieved and everything that is there, this is how I put my theory together.

Q. But from my work station, again, the logs are all in tact there and there is nothing in those logs, right?

A. From the host? No.

Q. And you keep saying could have been copied. You see no forensic evidence of that, right?

A. Not from --

THE COURT: I think we have trod this ground plenty. Move on, please.

BY MR. SCHULTE:

Q. You testified it was possible to copy the backup files in an hour, right?

A. Yes.

Q. And your presentation slides do not show the forensic basis for your conclusion, right?

A. No, there is no --

Q. OK. You did not establish network speed, right?

A. I'm sorry?

Q. In your slides you don't establish network speed, right?

A. No.

Q. You don't address the variables that degrade the network speed, right?

A. No, not in my network slides.

Q. A forensic expert cannot validate your claims, right?

A. Can you explain?

Q. Yes. A forensic expert has no idea what test you performed, right?

A. I think those tests might have been in my notes.

Q. I'm talking about your presentation, sir.

A. Oh no.

Q. Based upon your presentation a forensic expert cannot

validate any of your claims, right?

THE COURT: Sustained.

Q. Again, the forensic expert does not know what tests you performed, correct?

A. I disagree. I don't remember if they're in my notes or not.

MR. DENTON: Objection.

THE COURT: One at a time, and sustained. Let's ask a new question, please.

BY MR. SCHULTE:

Q. Your presentation -- in your presentation it does not reflect any tests you performed for network speed, right?

A. That's correct.

Q. In fact, there is nothing through your presentation for a forensic expert to analyze, all they know is your conclusion, they don't know your analysis at all, right?

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Take a look at your presentation. Can you show me where you analyze this?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. The fact that you do not even have a theory as to what device the data was copied to, this also impacts your analysis,

correct?

A. Can you define "impacts my analysis?" What do you mean by that?

Q. Yeah, sure. A theory of splitting the backup files across multiple drives or using slower drives obviously impacts the analysis, correct?

MR. DENTON: Objection.

THE COURT: Overruled.

A. To some extent it impacts the conclusion just because I would say I don't have the, like, an exhibit for that. To the extent I don't have an exhibit that affects my analysis, yes.

Q. Without knowing precisely what device or where information was copied, you can't say how long it would have taken, right?

A. Oh, I don't know, I disagree.

Q. You disagree? You can theorize how long something takes to copy without specifying what it is being copied to?

A. I think if it was taken -- so like the tests that I ran were based on copying to, like, a network location or just the file transferring of the network in general, so whether it was, like, copied somewhere quickly and, like, staged and copied later or something like that, I can't say, obviously, like I don't have a log of a certain USB device or a certain firmware number that I could test. No, I don't have that.

Q. I mean, if it is being copied to a tape drive it is going to take a long time to copy, right?

A. If it was being copied to a tape drive it would take longer than being copied to, like, a solid state drive. On a matter of principle, yes.

Q. Or how much data is being copied depends on your analysis too, right?

A. To some extent. I don't know exactly what you are getting at but I can say my copy estimate was based on the total size of Stash and the total size of the Confluence backups and, yes, it was very possible, in an hour time frame, more than enough to copy it.

Q. Based on the configuration of Deadline alone it would have taken at least four hours, correct?

A. I can't speak to that.

Q. Let's say at a speed of 100 megabits per second it would have taken four hours to copy 200 gigabytes?

A. Why would it only be 100 megabits?

Q. No, that's not the question.

A. Are you asking, like, from a mathematical standpoint?

Q. Yes.

A. Can you give me the numbers again?

Q. At 100 megabits per second it would take four hours to copy 200 gigabytes, correct?

A. It sounds close. I would want to run it through a calculator probably but that sounds somewhat close.

Q. I mean, we can walk through the math.

MR. DENTON: Objection, your Honor.

THE COURT: Sustained.

Q. So you said something about -- well, OK. Let's move on to the backups. It is fair to say that you don't know what DevLAN files WikiLeaks currently possesses, right?

A. No. I disagree.

Q. You have a contact in WikiLeaks?

A. No.

MR. DENTON: Objection.

THE COURT: Sustained.

Q. How do you know what files WikiLeaks has?

A. I mean I showed my presentation, the reasons why I believe that they have that March 3rd backup.

Q. You believe. You don't know, right?

A. Did you ask me if I believed? Yes.

Q. It is fair to say you don't know what DevLAN files WikiLeaks currently possesses, right?

A. Like I said, I have what I have presented. I don't have like a, you know, transcript from them saying this is the file we have but, I mean, there has been a lot of review done to show why that is the -- that is the backup file that was posted.

Q. I mean, all you know is what WikiLeaks was disclosed, right? That's all you know?

A. That's correct.

Q. So WikiLeaks could have files that you don't know about, right?

A. They could have all kinds of things, I'm sure.

Q. But based on the WikiLeaks disclosure, you know that at the very least they must have a copy of both Stash and Confluence, right?

A. Yes, and I don't know if it would need to be the entire Stash backups because I don't believe -- of the products released there were a handful of products released.

Q. Again, that's because you don't know what WikiLeaks has, right?

A. No, I don't have it. Like I said, I don't have a log of the exact files they have, just from the analysis of the, like, timelining of what backups are available, where things could have come from, and the points I made in the presentation.

Q. Just to be clear, the Stash and Confluence backups, they're digital files, right?

A. Yes.

Q. They're intangible, correct?

A. Intangible? Like, what do you mean by that?

Q. They're not tangible, hard copy documents; correct?

A. They're -- I mean, put them on a hard drive. Is that tangible? They're digital files.

Q. And you conducted an examination of the Stash, Confluence, and other Atlassian products' backups on DevLAN, right?

A. Yes.
Q. You are familiar with version control, right?
A. Yes.
Q. Version control literally keeps track of the edits or reversions of a file, right?
A. Yes.
Q. You are familiar with Git, right?
A. Yes.
Q. And Git is just a form of version control, right?
A. Yes, it is.
Q. And the Atlassian backups were essentially generated by simply copying all the data from the server into a single file, right?
A. Two files.
Q. Two files; a SQL file and the compressed file, right?
A. Correct.
Q. The TGZ file is the compressed file, right?
A. Yes.
Q. The compression is simply a way to reduce the file size without losing data, right?
A. That's correct.
Q. When the underlying Atlassian data from the servers is modified or deleted, a record of those changes is created, correct?
A. Yes; in the database.

Q. This allows a user to review all the changes over time, right?
A. For the most part, yes.
Q. This is sort of like tracked changes in Microsoft Word or in Google Docs, correct?
A. Yes.
Q. The user essentially has access to all prior versions of the data, right?
A. I believe so.
Q. And each successive backup contains the data of all the prior backups, right?
A. To some extent.
Q. There is some data that's not maintained through Git?
A. Are you talking about Stash or Confluence? They're kind of different.
Q. Well, both.
A. So I mean, like, using Git as an example you can definitely remove stuff from Git, like, prior commit history as an example. For Confluence I believe, like I showed in my presentation, if a page is deleted, that can be in the database still and be like marked as deleted.
Q. So all the data that was released by WikiLeaks can be found in every single backup starting with the March 3rd, 2016 backup all the way through the March 6, 2017 backup, right?
A. Is that like the most recent one that was in there?

Q. Well, I'm saying WikiLeaks released the data March 7, 2017, right? So the backup before that would contain the data as well, right?

A. I didn't do, like, the timeline, so I'm not sure exactly for that, like, that backup specifically. Like I said, you can change files in there, it is possible.

Q. Yeah. The question is just that the data released by WikiLeaks is found in all the backups from March 3rd, 2016 to March 6, 2017, right?

A. Sitting here today I'm not sure. It has been a long time since I looked at all of those but, like, from a general standpoint, they are version controlled so if you removed a page it would still be removed unless you unremoved it later. Stuff can change.

Q. Due to the version control feature the backups are going to contain all the data preceding it?

A. In a general sense.

Q. So if WikiLeaks received the March 6, 2017 backup file they had a choice of which one of the versions prior to the March 6 version they could release, right?

A. I disagree. I think it is a lot more complicated than just picking a date and saying revert the whole thing to this one date.

Q. I mean, you are familiar with Git, you said, right?

A. I think I really need to separate the Stash from the

Confluence because they do operate very differently from a technical standpoint.

Q. So for the Stash files it would have been trivial to do through Git, right?

A. It depends on what's there. Like I said, I didn't do a lot of the timing analysis for Stash, I focused more on Confluence. I probably did more Stash side of the house.

Q. I am talking about the Stash backups are based on Git, right?

A. That's correct.

Q. And you have knowledge in Git, right?

A. Yes.

Q. So if you have a commit log from Git all the way to March 7, 2017, right?

A. Assuming it is in tact and wasn't ever edited.

Q. OK, you could go back and select the commit from March 3rd?

A. You could. If it was there, yes, you could go back and --

Q. And Git makes this trivial to do, right?

A. It is easy to do.

Q. You testified that it may take some time to do this for Confluence, right?

A. Yes.

Q. And you also testified that sifting through the corrupt database would have also taken a lot of time, right?

A. Yeah. From my experience working with it, yes, it would

have.

Q. And according to you, WikiLeaks spent the time to retrieve content from the corrupt database, correct?

A. Yes.

Q. They exerted that effort to do so, right?

A. It appears so. From what they posted and what is in the database, yes.

Q. And from your investigation you learned about WikiLeaks, right?

A. Can you elaborate?

Q. I mean --

A. Like in a general sense?

Q. Yeah.

A. Yes.

Q. You learned, did you not, that WikiLeaks limits its release of data to protect its sources, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. As part of your investigation you wanted to learn how WikiLeaks released its information, right?

A. I mean, I have a general sense of what they posted in the past.

Q. You made an effort to learn how they did this in the past, right?

A. Yes, from -- just from reviewing, like, previous releases.

Q. And these releases would show you that WikiLeaks limits its release of data to protect its source, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. I want to talk to you now about the CIA's offsite backup. Backups from the Altabackup server were regularly taken off DevLAN and moved to an offsite backup, correct?

A. From what I understand, yes.

Q. All the backups were stored at the offsite backup, right?

A. The offsite backups were stored there, yes.

Q. And it is possible that WikiLeaks received the backup file from the CIA's offsite backup, correct?

A. I disagree.

Q. All right. Well, let's pull up what is in evidence as Government Exhibit 602 and this is page 2 of the document. Do you see the offsite backup site?

A. Yes.

Q. WMA storage; right?

A. Yes.

Q. Backups from the Altabackup server were regularly taken off DevLAN and moved to the offsite backup, right?

A. Yes.

Q. Did you conduct a forensic examination of the offsite backup?

A. Yeah, we had a -- I think we had a copy of that as well.

Q. No. Did you conduct a forensic examination of the site?
A. I have never been to the site.
Q. So no.
A. I can't really speak to the collection at the site because I didn't, like there is a cart -- the FBI forensics thing. I know that, like, reviewing, like, I had access to review the data stored from there but as far as specific questions for seizures, things like that at the site, physical stuff, I can't really speak to.
Q. So I mean, if someone stole the backup from the offsite backup and leaked them to WikiLeaks, you would have no knowledge of that, right?
A. I disagree; just from the -- I do know the security controls for the site and the fact that I think it was, like, a one-way transfer from, like, from DevLAN to the site and I --
Q. I'm not asking about someone from DevLAN, I am specifically asking about the offsite backup. If somebody stole the backups from the offsite backup and leaked them to WikiLeaks, you would not have any knowledge of that, right?
A. I mean, we have the like same file access time information from the main site that we do from the Altabackup share -- sorry, the offsite backup. So if those files were copied, that metadata would be changed in the same way that it is in what we have showed in the presentation so that's how I would determine whether something was copied there.

Q. You don't present any of that in your presentation though, right?
A. No. From what I understand it either, like, was an identical match to the data that we had or there wasn't any evidence of that type of thing over there.
Q. Would your analysis be any different if the backups were taken from the offsite backup?
A. If I was showing -- I would be showing something kind of similarly, like maybe an access time but I don't remember, honestly -- six years later now -- I don't remember the exact security requirements for accessing that site. I don't know if you could even, like, access the files that were there without physically being there. I don't remember.
Q. What about do you know if WikiLeaks received the backup file taken from COG through Hickok here?
A. I mean, it is my opinion that didn't happen.
Q. OK. Let's take a look at your presentation on page 11, and you can see here, like, on the other page Jira is connected to Hickok, right?
A. Yes.
Q. And you investigated the Hickok-Jira connection with COG, right?
A. To the extent, like I have reviewed the security plans for the firewalls that are in place there. The server itself, I don't know if it was re-purposed.

Q. So you reviewed technical documents about how it should have run?

A. That's correct.

Q. So DevLAN connected to the COG network here, right?

A. I don't see your cursor but if you are talking about the little bricks and the --

Q. Yes.

A. Yes.

Q. So if we can pull up Government Exhibit 601, which is also in evidence, this is describing the fire walls there, right?

A. Yes. This is one of the documents that describes them.

Q. Can you read the first, just that line there?

A. The confidential marked line?

Q. Yes.

A. The only traffic allowed into and from Hickok is HTTPS, SLDAP, SMTP, and SSH.

Q. Do you see that Hickok is set up to ensure SSH access; right?

A. Yes, but from only one side.

Q. SSH is a way to remotely access another computer, right?

A. Yes.

Q. Hickok permits SSH access, correct?

A. The firewall rules permit it. Like I said, I don't know about, like, if there were -- what was configured on the server specifically. I don't have a -- I don't have, like, the logs

from the server itself but from the firewall configuration, yes, SSH was allowed from either netware to the server.

Q. So someone from DevLAN can SSH into Jira, correct?

A. Yes. That's what I understand.

Q. And someone from COG can SSH into Jira too, right?

A. That's what I understand.

Q. And Jira mounts the Altabackups, correct?

A. So I believe so. The only issue is, like, NFS or, like, CIFS or --

Q. I am just asking if Jira mounts the Altabackups.

A. I know there are backups from Jira in Altabackup.

Q. And it needs access to Altabackups so it can store the Jira backups, right?

A. You can technically, like, SSH in and move them down. I don't know the frequency of the backups from Jira, I don't recall at this time so I don't know if it was something that were moved down over SSH or if it was set up in the same automated way that the other services were set up. I just don't recall at this point.

Q. Would Jira connect directly to the Altabackup server, right?

A. I can't say. Other than the fact that there are backups from Jira there I can't say the exact connection.

Q. Those backups are created -- their creation access and modified times show that they're being created and stored there

live, right?

A. Like I said, I don't know if they were, like, daily or if they were pushed in batches. I haven't looked at them in a while -- Jira backups anyway.

Q. So someone who logs into Jira could also then access the backups, correct?

A. If Altabackup was mounted, then theoretically yes.

Q. Someone from COG need only to SSH into Jira to access and copy the backup files, right?

A. If it was mounted. I can't speak to the exact state of it other than I know there were backups from Jira on Altabackup. Based on the firewall configs, like, NFS isn't explicitly allowed here so that presents an issue, but.

Q. I mean, you reviewed the Jira server, right?

A. Like I said, I think that server might have been re-purposed. I don't believe I have, like any -- I don't think I have any logs or anything from the Hickok server.

Q. But based on the directory Altabackup -- the Jira folder and the Altabackup directly, the fact that these files were being written there and from my work station it seems to indicate that this is the case, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. You reviewed my CIA work station, right?

A. Yes.

Q. You could see the logins to Jira, right?
A. There is an attempt I know, at least on 4-18 to log into Jira.
Q. Before that you know there were successful logins to Jira?
A. I believe so.
Q. And in the history files there there were -- it showed that the Jira mounted Altabackups, right?
A. I don't remember.
Q. In COG there is at least the same -- at least 200 people working COG, right?
MR. DENTON: Objection.
THE COURT: Sustained.
Q. Well, the individuals working in COG were experienced in using the malware tools, correct?
MR. DENTON: Objection.
THE COURT: Sustained.
Q. Are you familiar with what COG is?
A. Only so much that it's an operations group. I don't know -- I can't speak to their expertise or training.
Q. OK, but EDG writes the malware and sends it to COG to use it, right?
A. I know they are the customer for those tools.
Q. Nowhere in your presentation is there any slide about the investigation to access to the Jira server, correct?
A. No.

Q. Did you conduct any analysis of COG's network?
A. I did not personally, no.
Q. Did anybody?
A. I can't speak to anybody. I don't -- I know at least for myself I think the Bureau, I don't believe it was investigated.
Q. And why was it not investigated?
MR. DENTON: Objection.
THE COURT: Sustained.
Q. Based on your forensic knowledge of the way the systems were set up, COG could have access to the Altabackup server, right?
A. I disagree from the -- it's hard for me to say without having reviewed Hickok and the logs. All I can really speak to is the configurations, like, since I can't confirm the mount for Altabackup on the time. I know that those backups were there. Whether they were there over NFS from the share or whether they were, like, moved down over SSH is kind of all I can really speak to. If it was mounted to Altabackup and you could SSH into it, then.
Q. I mean, even if it was moved -- you keep saying if it was moved down through SSH, right? If it is moved down through SSH that is somebody actually running a copy command from Jira to copy those, right?
A. If you did it like that you would only have access to the backups that were like currently staged on the Jira server

itself, not all of everything in Altabackup.

Q. You are writing -- if you are copying files from Jira to Altabackup you have write access, right?

A. Well, you -- so, yeah, but you wouldn't be able to mount it over NFS if it was blocked at the firewall. That's the point I'm trying to make.

Q. Yes, but the firewall -- If the firewall is allowing SSH and Jira is mounting the directory and that's available to someone from COG, you could take those files, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. So I guess your testimony is essentially you don't remember or you don't know anything about the Jira setup?

A. Aside from what we just reviewed and the Jira backups that there are some Jira backups, I can't speak to the server configuration.

Q. That server configuration would have been very important in your forensic examination, right?

A. Yes.

Q. And you don't remember anything about it now?

A. No.

Q. OK. Let's pull back up Government Exhibit 602. There is also two foreign offices that are connected to EDG, right? To DevLAN?

A. Yes, from what I understand.

Q. Each of the foreign offices has a system that's connected to DevLAN, right?
A. I can't speak to the configuration. I know we received evidence from the foreign offices. That's really the extent of the foreign offices that I can speak to.
Q. This connection is established over the Internet, right?
A. I don't know, I can't -- I can't speak to the actual, like, network connection.
Q. You did not conduct a forensic examination of the system in the foreign office?
A. The work station? It was connected to DevLAN.
Q. You are saying that you don't know how this -- how it was configured?
A. I don't know how the networking configuration from DevLAN to the foreign office is set up. I just know that -- and from what I have been told and what we received from evidence from the office that there were some workstations connected to DevLAN from the location.
Q. So you don't know if this -- these connections were misconfigured or otherwise insecure, right?
A. I can't speak to the actual connection.
Q. It is fair to say that both adversary and friendly nations run cyber operations against each other; right?
MR. DENTON: Objection.
THE COURT: Overruled.

If you know.

THE WITNESS: In a general sense, yes.

BY MR. SCHULTE:

Q. And do you know that the United States has friendly nations and adversary nations, right?

A. I can't really speak to our foreign policy.

Q. I mean, do you know that adversaries to the United States try cyber operations against the United States?

A. Yeah. In a general sense, yes.

Q. And it is not unreasonable to think a foreign intelligence service might want access to DevLAN, correct?

A. DevLAN or other classified networks I'm sure.

Q. So if they breached DevLAN through these connections they would have the ability to copy the backups, right?

A. I can't really speak to that.

Q. You can't speak to the fact if they are able to breach DevLAN whether they would have access to information on DevLAN?

A. Well, I can't speak to the -- I don't know how anything about how that connection was set up, so.

Q. The question is if they were able to reach DevLAN would they have been able to copy the backups.

MR. DENTON: Objection.

THE COURT: Overruled.

A. So they would have the same type of, like, user access. It is a really theoretical question because at what level did they

breach it? Like, with what permissions? There is kind of a lot of open questions.

Q. Essentially you don't know -- since you don't know how the connections are set up you don't know if a breach is possible or what kind of access they would have, right?

A. No, not from that, from, like, the foreign office link I can't speak to it. I don't know the --

Q. OK. Let's move on to the home directories of the Altabackup server, Government's Exhibits in evidence 1207-60 through 63. This is the home directories, right, from DevLAN?

A. Yes.

Q. That's what all these exhibits are, right? Same thing?

A. Yes, same; home folders for users.

Q. I am going to show to the parties what's been marked as Defendant's Exhibit 1201. Do you recognize what this is?

A. Yes.

Q. And this is a document from -- showing information about DevLAN, right?

A. Yes, for the -- showing information about the file server.

MR. SCHULTE: I move to introduce 1201 into evidence.

MR. DENTON: No objection.

THE COURT: It is admitted.

(Defendant's Exhibit 1201 received in evidence)

BY MR. SCHULTE:

Q. So this is a listing of the shares on the Altabackup

server, correct?
A. I -- this is some of the shares. Like, I don't think Altabackup is in here because this is just the CIFS -- C-I-F-S -- shares.
Q. On the second page do you see where it says the "share name: Home"?
A. Yes.
Q. And the "group name: Everyone"?
A. Yes.
Q. What permissions does it give everyone?
A. Full control.
Q. What does full control mean?
A. You can create files, delete files, open files. Pretty much everything.
Q. So the DevLAN home directories were set up publically, right?
A. Home folder, yes.
Q. Anyone could copy files to each other's home directories, right?
A. I don't remember, like, the exact details. I remember hearing about that but I don't know how regular an occurrence it was.
Q. Through your investigation you learned developers regularly used this as a mail transport service with each other to transport data, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. Were you able to review what kinds of documents were stored on the home directories?

A. Yes.

Q. Based on those files, was it clear to you that this home directory is used as a transport?

A. I don't know if I call it a transport. I mean, people had this as storage for people to put their stuff. Yes, everyone could access it.

Q. So if you are on DevLAN and you want to send files to someone else, you can copy them to his share or you can say *Look at my share*. Right?

A. Yeah. With the permissions, you could do that.

Q. And we spoke very briefly about Dave C. and his lost drive, right?

A. Yes.

Q. Dave C. also stored a copy of Stash, the CIA's crown jewels, on his public home directory, correct?

MR. DENTON: Objection to form.

THE COURT: Sustained.

Q. Dave C. stored a copy of Stash on his public home directory, correct?

A. Yes. I believe there was a copy of Stash in Dave's home folder.

Q. And that's admitted exhibit 1207-85? This is a copy of Dave's home directory, right?

A. Yes.

Q. And you see the folder titled: Stash backup 4/16/16?

A. Yes.

Q. This is what is in the other directory, this is just named Stash, right?

A. It appears so.

Q. It is the SQL database?

A. Yes.

Q. I'm sorry 1207-86 in evidence.

And 1207-87 is also in evidence and this is the Stash backup, the 4/16-16 directory; right?

A. Yes.

Q. And that's Dave's directory, right?

A. Yes.

Q. And this is a full copy of the entire Stash data, correct?

A. It appears to be the correct size.

Q. The data released by WikiLeaks is contained in this file, correct?

A. I can't speak to that specific file. I don't know if I reviewed that specific file. Like I said, I did more Confluence review and less of a Stash review, but.

Q. But you know the Stash documents that were released predate April 16, right?

A. I don't remember the exact dates for the Stash, like, the timing analysis for Stash, but I believe so.

Q. Stash was much more valuable than Confluence, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. Stash contained the source code for all the CIA tools, right?

A. Contained the source code for tools developed on DevLAN.

Q. Right. And Confluence was just a wiki, as you testified about; right?

A. Yes.

Q. Stash contained much more sensitive data, correct?

A. I don't know the classifications of either. I mean, they were both sensitive things.

Q. But the source code and the amount of source code here -- 200 gigabytes -- is much more valuable than the small Confluence data, right?

MR. DENTON: Objection.

THE COURT: Sustained. Lets move on, please.

Q. There are also several other directories on the Altabackup server, correct?

A. Are you talking about the, like, the home folder and the source in gold folder or the --

Q. Yeah. There is many more directories or many more shares on the Altabackup server, right?

A. I believe there is a handful of shares.
Q. Just to be clear, the FS-01, that's the same thing as the Altabackup server, right?
A. Yes. So FS-01 is the server that has the home folders, all the shares we are looking at now, as well as the separate share for Altabackup. They are separate distinct things.
Q. As part of your investigation did you review these shares?
A. Yes, for what was available.
Q. You reviewed the OSB test repo, correct?
A. I think for the exact folders, I don't know what all from this list of permissions there were actual folders for, but if there was a folder on the server I reviewed it. I don't remember at this point, it has been a long time. I can only speak to the five folders I think at Exhibit 4 in the presentation. Those, I remember. Outside of that, I don't really remember.
Q. And every DevLAN user could access this test repo or DS-00 directory, correct?
A. I disagree.
Q. You don't think this test repo can be reviewed by everyone?
A. Well, everyone, you would have to have -- it needs to be on Windows.
Q. OK. Well, the permissions, I am talking access controls only.
A. Yes. As long as you are on the Windows part of the

network, yes.

Q. Each of these directories held copies of Confluence too, correct?

A. I don't know.

Q. You said you reviewed these directories, right?

A. I have never found copies of Confluence.

Q. And the OSB test repo or test 00 directory?

A. Like I said, I don't remember these other directories.

Q. OK. But from -- just from a forensic standpoint, you don't know if WikiLeaks received every single backup off DevLAN, correct?

A. I can't speak to what files they have, no.

Q. You don't know if WikiLeaks received every byte off DevLAN, right?

A. Like I said, I can't speak to the actual files they have.

Q. Right. So all you can say is that WikiLeaks disclosed information, right?

A. Yes.

Q. And that information was present in the backup starting with March 3rd, 2016, right?

A. So I can definitively say that the content posted on March 7 for Confluence came from that March 3rd backup, that specific backup.

Q. You found it came from the specific March 3rd backup?

A. From my analysis of it; yes, that's my opinion.

Q. If WikiLeaks received a March 4th backup they would have the same data, right?

A. From what I described I think it is highly likely they have the March 3rd backup.

Q. That's not the question, though. The question is backups after March 3rd, March 4th, March 5th, all those backups, WikiLeaks could have those, right?

A. Like I said, I don't know exactly what they have.

Q. And all you know is that WikiLeaks disclosed information starting up to March 3rd, right? The latest -- I'm sorry.

The latest data that WikiLeaks released is from March 3rd, right?

A. From Confluence, from what I understand, yes.

Q. So to your knowledge, the information released by WikiLeaks could have come from the offsite backup, right?

A. No.

Q. You said you didn't review the offsite backup?

A. No, I said I didn't --

THE COURT: I was just coughing but I think, Mr. Schulte, we have covered this ground, so let's move it to a new line, please.

Q. Based on the security logging and setup on DevLAN, the official offsite backup, the foreign offices, the links, there is absolutely no logging or mechanisms in place to trace who or when the data was copied, correct?

A. I can't speak to, like, all of those mechanisms. All I can say is that like I asked for --

Q. Yes.

A. -- network logs and never received any.

Q. Right.

So you didn't receive any of that because there is no security logs -- let's touch base real quick on the NetFlow logs.

MR. DENTON: Objection.

THE COURT: Let's let Mr. Schulte finish his question but, Mr. Schulte, I think we are kind of going backwards here. Let's go to new areas, please.

(Continued on next page)

BY MR. SCHULTE:

Q. OK. Just very briefly, the NetFlow logs, those logs would have shown data that was transferred along, across the network, right?

A. That's something they could have shown.

Q. OK. Let's turn to slide 29 in your presentation. You concluded that the data leaked by WikiLeaks must derive from one of the backups generated by the backup script, correct?

A. Yes.

Q. Slide 31 is the key points to the backup script, correct?

A. Yeah, it's -- this is why there was a corrupted database.

Q. This is the mySQLdump command, right?

A. Yes.

Q. And as part of your investigation, you analyzed the WikiLeaks data dump, right?

A. The release?

Q. Yes.

A. Yes.

Q. And you concluded that the WikiLeaks must suggest a malformed database file, correct?

A. Correct.

Q. That's this .SQL file, correct?

A. That's correct.

Q. In order to obtain a pristine database, the mySQLdump command had to be run in a special way, right?

A. Yes.
Q. But the command still required the passwords to the database, correct?
A. Yeah. You had to authenticate to the database to be able to export it.
Q. And these passwords were found in the script, right?
A. They're patched in as variables. They might be in the Python script that runs in the script.
Q. Yes. And these -- so if someone accessed the server, they could have simply run the backup script, correct?
A. If someone had access to the server, yes, they could have run the backup script.
Q. They could have copied this mySQLdump command and run that command, right?
A. Like, directly on the command line?
Q. Well, substituting variables and whatnot.
A. Yes.
Q. So in any case, your analysis does not conclude that the data released by WikiLeaks derived from a backup on the Altabackup, does it?
A. Part of that also includes the, you know, access times for those backup files.
Q. No. I'm just talking about this analysis, this analysis you ran here.
A. If you ran the mySQLdump command, it would create the same

kind of backup.

Q. OK. So in your presentation, you go through this entire section. The leak came from the Atlassian backups, and this entire section is based upon the script, right?

A. Yeah, the error that the -- that's introduced by this command is really important.

Q. But you can only conclude that the files released by WikiLeaks derived from a malformed SQL file, correct?

A. Say only conclude, but it definitely goes far to, like, assisting with the conclusion, yes.

Q. But this, based on your analysis, this is not -- this slide, 29, when you say the leak came from the Atlassian backups, right, this is not a conclusion you can reach from your analysis, is it?

A. I don't understand.

Q. If someone logged in to the Confluence machine and executed the mySQLdump command with the same command line arguments from the script, then the output SQL file would contain the same error, correct?

MR. DENTON: Objection.

THE COURT: Overruled.

A. Yes, if you ran that mySQLdump command, the -- I mean output file's going to be the same. It's the same command.

Q. And that output would not be an Altabackup file, right?

A. I don't understand. It's the same files that are on the

backup server. It's the --
Q. I mean your specific conclusion was that it came from the Altabackup directory, right; that was your conclusion?
A. This specific portion of the presentation is just to discuss the error with the database and why the WikiLeaks publication looks like it does and that it came from one of these corrupted backups, specifically the March 3 backup.
Q. We're just talking about this analysis. This does not have anything to do with March 3 right now, right?
A. I mean this -- all of this, part 2 is all about the analysis I did on that March 3 backup, so --
Q. But your analysis that you're running here is predicated on backups from the official Altabackup store, correct?
A. Yes.
Q. OK. So the point is if somebody accessed the server and ran this command, they could produce their own files, right?
A. Yeah, if you -- if you ran the mySQLdump command on March 3 at the same time as the one on the backup server, those databases would be, like, almost identical.
Q. So just based on this analysis, it's possible that WikiLeaks did not receive any backups from the Altabackups at all, correct?
A. I disagree.
Q. OK. So from this analysis, you can determine that WikiLeaks receives files specifically from the Altabackups

directory?

A. Sorry. Just having hard time -- like I said, the portion of this, talking about the backup script, the error, it's not so much about, like, whether it came from Altabackup. It's to date it and show that what they had was from a corrupted backup from that date. I don't really go to anything talking about, like, a page on WikiLeaks that shows, you know, like, where it came from.

Q. OK.

A. This specific stuff is just about that.

Q. So the question is simply not -- it's not whether you agree or disagree. The question is whether it's possible, based on the forensic analysis of the script, that WikiLeaks received files that were not from the Altabackups.

A. I -- I can't speak to, like, exactly what they have, so -- I -- I'm just trying to say that if you ran the dump command, it would be the same database that's on the backups.

Q. OK.

A. Whether it -- yeah, go ahead.

Q. This is just the point. The point is you run this command, you get a file, that file's not one of the official backups, right?

A. If you ran the command on the server, yes.

Q. OK. And then that file got transmitted to WikiLeaks, correct?

A. I don't --
Q. This is a possibility, right?
A. We're talking about a theoretical scenario.
Q. Yeah. I'm just saying is it possible. That's the question.
A. You could make a new backup if you had access, like, to the server. Like, you could run these commands. As long as you had permission to access the database, yes, you could run the backup script.
Q. OK. So based solely on your analysis on this backup script, right, it's not forensically possible to determine whether WikiLeaks received the file from the Altabackups or not? Right?
MR. DENTON: Objection.
THE COURT: Sustained.
BY MR. SCHULTE:
Q. OK. Based on your analysis on this, on the backup script, right, your analysis of the corruption of the SQL file, that's the conclusion that you made? Right?
A. Yeah, and also reviewing the Confluence --
Q. No. I'm just asking about this. I'm just asking about your analysis on this specifically. We'll move on to the next part later.
A. Yeah. The post on WikiLeaks came from a corrupt database. That's my testimony, and that's sort of -- that's what this is

meant to show.

Q. OK. And based on this, it's not forensically possible to determine whether WikiLeaks received the file from Altabackup, right?

MR. DENTON: Objection.

THE COURT: I'll allow it. Overruled.

A. So, the forensics, like, for this theory that we're talking about now --

Q. It's just yes or no.

A. Can you rephrase the question? Or just restate would be fine.

MR. SCHULTE: Can the court reporter reread it, please.

THE COURT: The question is "based on this it's not forensically possible to determine whether WikiLeaks received the file from Altabackup, right"?

A. No. I disagree.

Q. You just said that somebody can run this command separately, correct?

A. Yes, in this theoretical scenario, there would be additional logs for this command being run, especially --

Q. We're just talking about the possibilities here.

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. You testified that someone can run this script and produce their own file, right?

MR. DENTON: Asked and answered, your Honor.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. Sir, it's possible, correct, that WikiLeaks received a different corrupt database?

A. I'd say no.

Q. Based on this analysis alone.

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. This analysis you did on the backup script, right --

A. So --

Q. I'm just talking about this analysis. We'll talk about the other thing later.

A. I don't think talking about this is enough to qualify that statement. There's a lot of other things you need to take into account.

Q. Like what?

A. On the Confluence server, especially on March -- March 3, there's -- there would be logs and history, command history or even, like, in unallocated space, for, like, this type of command being run, and we know this command would have had to

have been run on March 3 to make the same backup, so there's -- there's no evidence of that.

Q. Well, you don't know that the March 3 backup was stolen, correct?

A. I don't understand. It --

Q. You've testified that the backups after March 3 contained the same data, right?

A. It could.

Q. OK. So you can't say that it had to be -- the command had to be run on March 3, right?

A. I think I go a long way to showing that with this part of the presentation. I --

Q. If someone on, you know, in December accessed the server and ran this command, it would contain the same data WikiLeaks had, right?

A. It could potentially have the data from before.

Q. OK.

A. It's -- I don't think you'd be able to, you know, make an accurate one-to-one, like, March 3 copy without actually having the March 3 copy to, like, compare from. Just from what was missing in that database, I just don't think there's enough information there.

Q. I thought your testimony on direct was that it was possible; it would just take work.

A. Yeah, it would be a significant amount of work. I think --

Q. That's all I'm asking. It's possible, right?

MR. DENTON: Objection, your Honor. Can the witness finish the answer?

THE COURT: Sustained.

Go ahead, Mr. Leedom.

A. Yeah, and something that would be a big part of that would be, like, having to have that older backup. I think from, like, looking at what we reviewed and that it was clear they tried to get every morsel out of what was in there. So, in my opinion, if they had a later backup, we would see every morsel of what was in there from a later date, not from March 3.

Q. That's just your speculation, though, right?

A. My opinion.

Q. Because, like you said, you don't know actually what files WikiLeaks had, right?

A. I don't know exactly what files were on their server, no.

Q. And you testified they tried to get every morsel of data out of March 3, right?

A. My opinion.

Q. Right. So if they had a later backup and they restricted themselves to March 3, it would be the same, right?

A. Well, if you're restricting yourself, you're not getting every morsel out of it.

Q. Well, you'd get every morsel out of the March 3 data, right?

MR. DENTON: Objection.

THE COURT: Sustained.

We've covered this plenty, Mr. Schulte. Let's move on before I cut you off altogether.

MR. SCHULTE: All right. Let's look at slide 26.

Q. Just to be clear here, opening a file automatically updates the access time, correct?

A. You said opening a file?

Q. I'm sorry. You didn't hear?

A. Did you say opening a file?

Q. Opening a file updates the access time, right?

A. Yes.

Q. OK. Access time only tells you one thing, correct?

A. Could be multiple things but this tells you last time the file was opened for reading, yes.

Q. The access time only tells you the file was accessed, right?

A. That's correct.

Q. Does not forensically indicate that the file in question was copied, correct?

A. Other than that you can read what's in it, no.

MR. SCHULTE: So let's take a look at -- one second.

Q. So you're -- there's no forensic artifact to support the notion that those specific files from Altabackup were ever provided to WikiLeaks, correct?

A. Other than the step we've talked about previously, there's no forensic artifact of, like, a copy command for those files, no.

Q. Do you know about the Linux touch command?

A. Yes.

Q. This command can be used to change file times, right?

A. Yes, it can.

Q. That includes access times, right?

A. Yes.

Q. And from reviewing my workstation, you know that I developed Linux malware tools for the CIA, right?

A. I know you worked on a few tools. I don't know if they were Linux-specific or not, but --

Q. And you knew from that that I wrote malware that specifically used the touch command to change file times, right?

MR. DENTON: Objection.

THE COURT: Overruled.

A. I don't know about the specifics of the code you wrote.

Q. You did not review any of the source code?

A. I reviewed -- it was a long time ago, and like I said, I didn't review, like, every single project either.

Q. OK. But would you not agree that malware developers know how to change file times?

A. I can say sometimes malware time stomps files.

Q. OK.

THE WITNESS: Time stomp, that's what we call it.

I can explain.

THE COURT: Go ahead.

THE WITNESS: So, when, like, a malicious actor or malware, usually when they're, it's, like, when they're cleaning up, they will change file time stamps for files to make it look like, you know, if they edited a file; they'll make it look like it was edited on an earlier date. In the field, that's called time stomping.

BY MR. SCHULTE:

Q. And it would take only a few seconds to type a touch command to replace the access times, right?

A. It's a short command.

Q. And in fact, Windows also has a very simple command to change file times, correct?

A. I think it's a bit more complicated in Windows.

MR. SCHULTE: All right. I'm going to show the, just the parties and the witness what's marked as defense exhibit 1206-1.

Q. And do you know what this is?

A. Looks like a API, Windows API call.

Q. And what does Windows API mean?

A. Programmatically, if you want to perform an action on Windows, there's a set of, kind of predefined, we'll call

functions that you use that will do that for you. So this is one of those.

Q. So when writing source code, you use Windows API to do that, right?

A. Yes. This would be something you have to, like, actually write out a program to do.

Q. And Windows documents all their calls so that developers can use them, right?

A. Not all of them, but there are most that are documented.

MR. SCHULTE: I move to introduce 1206-1.

MR. DENTON: Objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. Well, you recognize what this API is, right?

A. I mean I can -- I haven't used it. I can read the description, what it's for.

Q. And this is a technical document, correct?

A. Yes.

Q. It describes how technical code can be used, right?

A. Yes.

MR. SCHULTE: Now can I move this into evidence?

MR. DENTON: Same objection.

THE COURT: Same ruling.

Let's keep going, Mr. Schulte.

BY MR. SCHULTE:

Q. OK. Are you aware of a function in Windows to change file times?

A. Yes, I know it's possible.

THE COURT: Let's take this down, please.

MR. SCHULTE: I'm just going to show the witness what's marked as 1206-2.

Q. And Windows, just like in Linux, it's -- there's a function call to change the times, right?

A. So, in Linux, you're talking about a command that you would run, like a touch command that you'd run. This is, like, something you'd have to write a program for. It's different.

Q. OK. But it's one command, relatively short to do it, right?

A. I think writing a program to achieve this is a lot more effort than typing, like, the touch command, for example, but --

Q. OK. But it would be a very small program or very -- it wouldn't take very many lines of code to do it?

MR. DENTON: Objection.

THE COURT: Sustained.

Let's move on, Mr. Schulte.

BY MR. SCHULTE:

Q. If an intruder noticed the April 20, 2016, access time on the March 3, 2016, backup, they easily could have chosen to

release files from March 3, 2016, to WikiLeaks to plant a false flag, correct?

A. I can't speak to the, like, the -- I don't know, like, what an intruder's thought process would be.

Q. It's just if it's possible.

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Do you know what a false flag is?

MR. DENTON: Objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. As part of your experience, training, investigation, do you know or have you researched the false flags?

MR. DENTON: Objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. During this investigation, did you look for false flags?

A. To the extent that you can, like, look for false flags, I mean it's -- any kind of unauthorized, like, access to the network would be something we looked for.

Q. I'm sorry. So your testimony is you looked for them as much as you could?

A. From what we, from what evidence we gathered, it was, you know, it's part of something you -- you analyze evidence with. If you see, like, if there, like -- there wasn't any, but if there was, like, an event where someone had accessed the network, then, yeah, you would review, like, where that came from and, like, try to make some sense of the reasons behind it. Like, to the extent you're looking for a false flag, that's what you would do, but from our review, we never found anything that would indicate that.

Q. But false flags generally are difficult to discern, correct?

A. Not always.

Q. Have you heard of the Olympic Destroyer malware that disrupted the Olympic Games in 2018?

MR. DENTON: Objection. Relevance.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Through your position and expertise, you research and learn about operations that are occurring in the wild, correct?

A. I do.

Q. OK. So based on your expertise and experience, did you know about the Olympic Destroyer malware from 2018?

MR. DENTON: Objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. Did you know that malware used false flags to mislead reverse engineers?

A. Yes.

Q. And you're a reverse engineer, correct?

A. I've done reverse engineering in the past.

Q. And from your review on this case, did you know it was common practice at the CIA to plant false flags?

MR. DENTON: Objection.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Did you know every developer on DevLAN had training in miss --

MR. DENTON: Objection.

THE COURT: Sustained.

Let's move on, Mr. Schulte.

BY MR. SCHULTE:

Q. You testified on direct about the snapshot from April 16, 2016, right?

A. Yes.

Q. And I think that's slide 68 in your presentation.

MR. SCHULTE: Pull that up.

Q. This snapshot was named BKUP 4-16-2016, right?

A. Yes.

Q. And BKUP is a common nomenclature for backup, right?

A. I don't know how common it is. I think it's clear it stands for backup.

Q. OK. Did you check whether the Confluence backup access time was a direct byproduct of the Confluence snapshot itself?

A. It was not.

Q. Did you investigate that?

A. Yes.

Q. Did you replicate the DevLAN network?

A. You can't replicate the DevLAN network.

Q. You couldn't replicate the DevLAN network?

A. No.

Q. Why?

A. I mean by the time we got there, it was a year after this time frame, and there had been a lot of changes to that network.

Q. You were aware that Dave C. and Jeremy Weber took the April 16, 2016, snapshot, correct?

A. Yeah, that, that weekend. I think it was -- I don't know which one of them did it, but --

Q. If they initiated a process or cron job that ultimately touched the March 3, 2016, backup file, it would have been preserved in the snapshot, right?

A. Before or after they took the snapshot?

Q. Well, before, during.

A. If they ran a cron job to -- if they ran a cron job before

taking the snapshot -- well, yeah, they didn't do any reversion, so, yes. I don't remember seeing anything like that from my review.

Q. The question was just would that be preserved in the snapshot?

A. If it happened before the snapshot was taken, yes.

Q. So in this case, on April 16, 2016, the March 3, 2016, backup would have been accessed, correct?

A. No.

Q. It wouldn't have been?

A. I don't understand. This is just a snapshot that's being created. This has nothing to do with the backups or anything.

Q. Well, the question is if they initiate a process or cron job that ultimately touched the file, then it would have been accessed on that day, right?

A. I can't speak to, like, the theoretical if they did something. I -- reviewing the machine I did not see anything like that.

Q. Just forensically, is this possible?

A. At any point if you access the file, the access time would change.

Q. OK. So if this was preserved in the snapshot on April 16, it would have updated the access times, right?

MR. DENTON: Objection to form.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. Is it possible forensically that the process or cron job was initiated prior to the snapshot on April 16, 2016?

MR. DENTON: Objection to form.

THE COURT: Sustained.

I'm not sure I understand the question, Mr. Schulte.

MR. SCHULTE: OK. So let me just go back and ask this question.

Q. Jeremy Weber and Dave C., if they initiated a process or cron job that ultimately touched the March 3, 2016, backup file, it would have been preserved in the snapshot, right?

THE COURT: That we've already covered, so a new question.

MR. SCHULTE: OK.

Q. So in that case, then on April 16, 2016, the March 3, 2016, backup would have been accessed, right?

A. If they did that and it was accessed on the 16th, then the access time would be for April 16.

Q. Yes.

A. But the access time's not April 16. It's April 20.

Q. I understand that, but -- OK.

And if that were the case, the next question was you'd expect the March 3, 2016, backup to show an April 16, 2016, access time, right?

A. If they accessed it on the 16th, then yes.

Q. OK. So when the Confluence was reverted back to the April 16 snapshot, it would have executed the same cron job and touched the March 3, 2016, Confluence backup file again, correct?

MR. DENTON: Objection. Compound, hypothetical, your Honor.

THE COURT: Sustained.

BY MR. SCHULTE:

Q. So when Confluence was reverted back to the April 16, 2016, snapshot, it would have executed the same cron job, right?

MR. DENTON: Same objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. OK. Let's talk a little bit about the permission change in the April 16, 2016, snapshot. All right? On the next slide, 69, shows a list of authorized SSH keys before the snapshot, right?

A. That's correct.

Q. And 70 shows that all the SSH keys were removed, right?

A. Yes.

Q. And then a new one was added, right?

A. Yes.

Q. And the only way you concluded that the April 16, 2016, snapshot maintained my previous privileges is by actually

reverting to the snapshot, right?

A. Yes. We have the snapshot.

Q. But you would agree that there would be absolutely no way for anyone to know the state of the virtual machine in the April 16, 2016, snapshot, right?

A. There -- I mean I think I -- I can't speak to what everyone knew on the network, but wasn't there an email that was -- that said, like, the changes happened that weekend?

Q. No, no. The question is there's no way to see what permissions exist in the snapshot, right?

A. Without -- you'd have to go into the snapshot and, like, view the system at that time.

Q. You'd have to actually execute the snapshot -- you'd have to revert to the snapshot, right?

A. If you wanted to look at files from that snapshot, yes.

Q. If you wanted to see what accesses were in that snapshot, right?

A. There would be the file in the snapshot.

Q. OK. So this, your slides here, 69, 69 and 70, you don't know this information from the snapshot, right?

A. Like, looking at the -- I'm confused. The data in the snapshot?

Q. No, no.

A. Or --

Q. Yeah. I'm sorry. So outside. Without looking, without

running the reversion, you don't know any of this, right?
A. The only thing you know about the snapshot without reverting the snapshot is what's in the, like, I don't know if it's the previous slide, where it shows the snapshot information, just, like, a time stamp and name, things like that. That's all you'd know about the time stamp -- or the snapshot.
Q. OK. And then once you revert it, then that's when you could learn the privileges changes, right?
A. Yes.
Q. Have you ever been a system administrator before?
A. I have in some capacities.
Q. Have you ever managed Enterprise system with multiple virtual machines?
A. Yes.
Q. So you know the process of taking a snapshot is a common system administration, correct?
A. Yes. I think I've said that too in previous testimony.
Q. OK. Taking a snapshot's not an inherently harmful computer command, correct?
A. No.
Q. The process of reverting a snapshot is also a common system administration, correct?
A. In some circumstances, yes.
Q. Just whether this is common in system administration.

A. It's something that you would do for certain reasons.
Q. And reverting a snapshot is not an inherently harmful computer command, correct?
A. It's harmful to the state of that machine. If you revert to a -- if you have a snapshot from one month ago and I revert, then I'm going to lose everything that happened for the last month, so it is a -- I don't want to use the word "destructive," but it is a -- it will, you know, delete that information.
Q. But it's still, it's still common to run this in system administration practices, correct?
A. Like I said, for some instances, yes, you would revert a virtual machine.
Q. If you're going to, if you need to roll back a system, right?
A. Yes.
Q. And deleting a snapshot is not an inherently harmful computer command, correct?
A. No.
THE COURT: All right. We're going to take our break now.
Ladies and gentlemen, a couple standard reminders.
Don't discuss the case. Keep an open mind. Don't do any research about the case.
It's 11:40. Let's get going promptly at 12:20, so

please be ready to go beginning at 12:15.

With that, I'm going to excuse you. Enjoy your break. Thank you.

(Continued on next page)

(Jury not present)

THE COURT: You may be seated.

Mr. Leedom, I remind you that you shouldn't discuss the substance of your testimony with anyone from the government during your break since you remain on cross. Please be here or be in the witness room by 12:15 and ready to go.

THE WITNESS: Yes, sir.

THE COURT: With that, you may step down.

Mr. Schulte, any estimates of how much longer you have? I have to say the pace of this I'm finding quite difficult.

MR. SCHULTE: Yes. I'm trying to touch on everything.

THE COURT: I'm just asking for a time estimate.

(Witness not present)

MR. SCHULTE: Yeah. I mean from this, I have, maybe, half of what we've gone through already. So from, we start 9:30 to 12, half of that, an hour and a half or two hours, maybe.

THE COURT: OK. I would really urge to try to pare things back. First of all, I think a lot of the technical details are completely lost on the jury. I think there's a lot of repetition, a lot of questions that are being asked and answered multiple times, and I'm just going to start forcing you to move along. It's just not a tolerable pace and I don't think you're making a whole lot of productive use of the time

you're being given other than establishing that there's no forensic evidence of codes copied with external drives or anything of that sort. It's just not clear to me what you've accomplished in most of this cross, so I'm going to start to force you to use your time a little bit more wisely and valuably.

Anything to discuss before I give you your breaks?

Mr. Denton.

MR. DENTON: Not from the government, your Honor.

THE COURT: Mr. Schulte.

MR. SCHULTE: No.

THE COURT: All right. Please be back by 12:15, and we'll get going promptly. Thank you.

(Luncheon recess)

A F T E R N O O N S E S S I O N

12:15 p.m.

(Trial resumed; jury present)

THE DEPUTY CLERK: Jury entering.

THE COURT: Welcome back, ladies and gentlemen. I hope you enjoyed your break. We will continue with the cross-examination of Mr. Leedom.

You remain under oath, Mr. Leedom.

THE WITNESS: Yes, sir.

THE COURT: Reminder, again, to please move the microphone closer, speak slowly, clearly and into the microphone. And, you may remove your mask.

You may proceed, Mr. Schulte.

BY MR. SCHULTE:

Q. Before we went to lunch we were talking about snapshots and reversions and system administration. As part of your investigation you stated that you reviewed my CIA workstation, correct?

A. Yes.

Q. And through your investigation -- I'm sorry. Let me restate.

And your investigation revealed that I regularly took snapshots and reversions, correct?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. In your investigation of all developers' systems did you determine that snapshots and reversions were common and regular practice on DevLAN?
A. I don't recall, really, the exact frequency. I mean, there were developers that used virtual machines and I assume had snapshots but I can't speak to their, like, normal everyday practice, really.
Q. Let's discuss the reversion for a minute. A reversion is when you go back to a point in time, correct?
A. Yes, a point when you go to a previous snapshot.
Q. And during the time you are in a reversion, the system itself is still running, correct?
A. No.
Q. When you are in a reversion the system is not running?
A. Are you talking about, like, the process while it is reverting? Or --
Q. No, once you have done the reversion. Once you executed the reversion the system is still running, right?
A. If the snapshot was taken while the system was running it would be just as it was when the snapshot was taken.
Q. And others who may be unaware of the reversion are still working on their projects, right?
A. I don't understand.
Q. So other people who are working on Confluence, they would not know that there has been a reversion, right?

A. From what I understand, the way that system worked there wasn't any of the -- there are -- let me explain this. So there are features of certain versions of ESXi that support -- I don't know what the term is but a type of reversion where if a user was using the system they wouldn't notice but in this case, like, if you were currently trying to edit a page and then it got reverted, you would have to log back in again.

Q. So if changes are being made this would be noticeable, right?

A. Can you explain?

Q. It is fair to say that anyone who worked on Confluence documents during the reversion period would lose their work that they added when the system reverted back to the present state, right?

A. I believe so. Yeah.

Q. It is fair to say that a person would realize that data would have been lost by the reversion, correct?

A. Yes.

Q. Confluence documents were on the DevLAN system, correct?

A. The Confluence server was on DevLAN.

Q. And DevLAN was accessible from at least two different vaults, correct?

A. I don't know exactly how many or which vaults, but yes.

Q. There is one on the eighth floor, right?

A. I don't remember which floor.

Q. But you don't, through your investigation, you didn't learn what floors DevLAN was on?
A. I did during the investigation but today I just don't remember.
Q. But you know there were at least two different floors that this was on, right?
A. I believe there were multiple floors that the group operated on.
Q. And you testified on direct that there were about 200 employees in all this DevLAN space put together, correct?
A. Yes, about 200.
Q. And you were at the CIA during your investigation, correct?
A. Yes.
Q. For months at a time, right?
A. Yes.
Q. And you observed how the CIA employees worked, correct?
A. Which employees?
Q. The developers.
A. No.
Q. You didn't work with any of the developers at all?
A. I wouldn't say any but, like, we were very much -- what's the word -- like isolated from all of the people and developers for DevLAN. I think there might have been one or two developers that we spoke to for, like, for some questions, but not like any kind of regular contact.

Q. OK. But through your investigation into the forensics, you learned that developers typically worked well past 5:30, correct?

A. People had different schedules. Some people worked later.

Q. I mean, you know that working for the CIA isn't a 9:00 to 5:00 job, right?

A. Correct.

Q. And that at 5:30 p.m. on April 20th, there were at least 15 developers still working in the vaults, right?

A. I don't remember.

Q. You don't remember how many people were actually in the vaults on April 20th?

A. Not at this time. The only thing I remember from that metric is the vault that you closed. I don't remember the details from the other vaults at this time.

Q. Well, performing a snapshot and reversion at 5:30 would have been very noticeable, right?

A. It depends.

Q. You just testified that people would know that their products aren't being -- the work would be lost, right?

A. Only if you were, like, editing or updating a page on Confluence.

Q. So if you were working during this time this would be noticeable, right?

A. It really depends on what you are doing. If you are just

viewing a page an hour is not a super long period of time, even in a work day.

Q. You said you would have to log in again, correct?

A. Yes. It would probably ask you to, re-prompt you for login which depending the last time you have logged in may not be very noticeable or expected.

Q. It certainly would have been noticed unless there was a heads up sent out about it, correct?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. Typically, in system administration you would send out a notice before doing something like this, right?

A. Yeah, making some kind of a, like a change like that, that's going to happen while users are using the system, that would be something that I think would be normal practice.

Q. Because this is the Confluence system, it is a production system, right?

A. It is.

Q. And in the course of your investigation you learned that there was a chat feature in Confluence, correct?

A. I think there was, like, a comment feature.

Q. No, I'm talking like instant messaging feature.

A. I don't remember an instant messaging feature in Confluence.

Q. You don't recall individual users sending messages on the

system?
A. I know there was an IRC chat on the network.
Q. But you don't recall any chat feature that was actually in the web browser for Confluence?
A. Not that I remember at this time.
Q. That would have been part of your investigation, right?
A. Yes. If there was content from that that was relevant I would have reviewed it.
Q. So through your investigation you don't recall any message -- global message going out about the Confluence system?
A. There was an e-mail that was sent about the migration that was going to happen on the 25th, but.
Q. No, I'm talking on DevLAN; through your investigation, did you not learn that there was a global message sent about the Confluence downtime on April 20th?
A. No, I don't -- I don't remember.
THE COURT: You don't remember at all or you don't remember there being such a message?
THE WITNESS: I don't remember there being such a message.
BY MR. SCHULTE:
Q. You testified that deleting the April 20th, 2016 bkup snapshot on the system, right?
A. Yes.

Q. OK.

A. Or -- excuse me. No, not the 4/16 snapshot.

Q. The snapshot, the name was bkup?

A. Just bkup.

Q. Yeah, so you testified that deleting this snapshot, bkup, deleted data on the Confluence system?

A. The process of reverting and deleting it, yes.

Q. I'm just talking about just deleting the snapshot?

A. If you just delete the snapshot in a vacuum while you are running past it, as long as you are past it then it deletes the mile marker but no content from that is deleted as long as the system is still running. It is the reversion portion that really creates the deletion.

Q. So I'm just saying the deletion of the April 20th snapshot did not delete any data from the system, right?

A. No. No, just deleting the snapshot itself after you have reverted to it, that doesn't remove anything. It is the reversion portion that does the deletion.

Q. And the deletion is not -- it is just inherent to the reversion process, right?

A. No. You have to specifically delete it. When you revert it doesn't, you know, it doesn't even automatically say, like, delete, it is just you revert it and then you have to manually go in and delete it afterwards.

Q. I'm sorry, no. I'm talking about when you do, when you

revert -- when you actually execute a reversion to another snapshot, right, the loss of data is inherent in the reversion itself, right?

A. Yes.

Q. So you are not actually going through and deleting files or anything like this, right?

A. By the process of reverting you have deleted everything, not just files, but everything that's happened in the last however long it was.

THE COURT: In other words, just to translate, when you revert to an earlier backup you would lose any changes that were made between the time that that snapshot was initially made and the reversion to snapshot; is that correct?

THE WITNESS: That's correct. It also works the other direction as well.

THE COURT: What do you mean by that?

THE WITNESS: So in this case we had created a backup at the current time and reverted to an old one and then did some stuff and then reverted back to the current one. So that period of time that is sandwiched in between there is what gets erased.

BY MR. SCHULTE:

Q. I want to move on and show your slide presentation on slide 82. Shell history or bash history typically records input like this, right?

A. The commands that are run, yes. The shell.log and ESXi is a little more verbose.

Q. But the point is you are recording -- these files record user's input to the system, correct?

A. Yes; commands that were executed.

Q. ESXi, like you said, specifically writes the commands to a shell.log file, right?

A. Yes.

Q. But by default it does not record the output of the commands, correct?

A. That's correct. I don't even think you can configure it to do that.

Q. That's right.

Let's turn to slide 116. So this is not normal system logging, correct?

A. Correct.

Q. This shows command input and output, correct?

A. That's correct.

Q. And these are known as transcript files, correct?

A. That is one method that this data could be logged, yes.

Q. And you testified at length about these transcript files from my CIA work station, correct?

A. Yes, about these, yeah, the logs that we have shown here.

Q. Let me take it down and just show the witness what has been marked as Defendant's Exhibit 1207. This is an online manual

page, right?

A. It appears to be.

Q. And you know that Linux has a script command, correct?

A. I don't think I have ever used it, but reading the page it seems like --

THE COURT: This isn't it evidence so don't read what is on this page. Just answer based on your knowledge, please.

A. I haven't used this specific command but seems likely, yes.

Q. But the script command creates transcript files, correct?

A. Like I said, I haven't used it. I can look at the documentation and explain from that but I haven't personally used it. I'm not sure that I am allowed to say here.

MR. SCHULTE: I move to introduce this Exhibit 1207.

MR. DENTON: Objection.

THE COURT: Sustained.

Q. You testified that you are familiar with system administration, right?

A. Yes.

Q. And that you have managed large servers before, correct?

A. I have managed servers before.

Q. And it's common practice for a system administrator to record their actions to keep a record for other system administrators, correct?

A. It depends.

Q. I mean, you want to record if something goes wrong, right?

A. It really depends on what your individual policies are on the network and who you are working with and what types of systems you are working on.

Q. OK. But it's good practice to essentially record actions taken on enterprise systems, correct?

A. Yes.

Q. And system administrators do this through the script command, correct?

A. Like I said, I haven't used it but if a script command, you know, could create a log of that then, yes, I suppose you could use it for that but I haven't personally used it.

Q. I am going to bring back up the 1703. This script command is the one that generates transcript files like these, correct?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. Is one way to generate files like this to use the script command?

MR. DENTON: Objection.

THE COURT: I will allow it.

A. I'm not familiar, like I said, with the exact output of the script command, but.

Q. So to your knowledge, how were these files created?

A. So I know you can have, like, command logging enabled for the terminal session itself and there is various ways that things like this displayed on the screen can eventually end up

on disk. Like I said before, since we were looking at this, like, the year afterwards, I wasn't surprised to see something like this and, like, for the script command, I don't remember -- I don't recall ever seeing script command run in this time frame looking at command history on the machine either. So there is various different ways this information could show up.

Q. But you don't recall there being any other transcripts on my CIA workstation except from April 20th, correct?

A. I mean, there are similar artifacts to this from -- I believe, like, from the 18th.

Q. But I mean there is no, from April 20th until I resigned in November, there is no other files like this on the system, correct?

A. So this isn't, like, a file, really, this is a portion of space that was on the virtual machine that is marked as unallocated, it doesn't have any relationship to, like, an individual file or files for that matter. This is essentially just data that's remaining on the disk, so.

Q. Yeah. The question was did you see any file or any data like this on the workstation from April 20th until I resigned in November?

A. I don't know the absolute last timestamp entry or anything from that machine. This activity was presented for being in the April 20 time frame. I don't know or remember what was

there from after that.

Q. But the only reason you have these files to exhibit here is because the script command or other user intervention was used to record this data, correct?

A. No. I can't say that at all.

Q. Then how was this file created?

A. I can't say that it was from user intervention. I mean, just the way computers operate what can end up in memory from using a terminal session or if it is saved to a file, things get saved to disk. I really can't say.

Q. But normally -- you agree, normally, you don't see output like this, correct?

A. Correct.

Q. And the terminal itself does not log that, correct?

A. You can configure it, too.

Q. That would require user intervention, correct?

A. Yes, you can say that.

Q. You testified on direct that when somebody does something nefarious or deletes documents that that's what you called a clue for your investigation; correct?

A. Yes.

Q. So wouldn't the fact that an individual purposefully recorded a session also be important to that analysis?

A. It would be but, like I said, I don't have any evidence of that.

Q. OK. So your testimony is that you simply don't have any idea about how or why these files were created?

A. No.

Q. All right. Let's move on to slide 62. So my key was never removed from the ESXi server, correct?

A. That's correct.

Q. And it was on the ESXi server from the time I set it up in 2014 until the time I left the agency in November 2016, right?

A. I don't know the exact first date that it was -- it would have been on there but I know it was there when it was seized so it was still there.

Q. It was still there a year after I left?

A. I believe so.

Q. And this key is sitting on the ESXi server in plain sight, right?

A. The public key? Yes, it is an authorized keys file.

Q. There is no attempts to hide it, correct?

A. It's a normal file that's used for operation, so.

Q. And accessing a server using a key is very common, right?

A. Yes.

Q. Basically the same as someone using keys to unlock and open their front door, right?

A. That's correct.

Q. And from your forensic examination you confirm that I always logged into the ESXi server using my key, right?

A. I don't remember if every single login was SSH only. I just don't remember but I know on the 20th you did -- well, I guess on the 15th you did.

Q. Well, the way it is set up, just by running the SSH command it automatically uses the key, right?

A. When you say "it" you mean like --

Q. If you run SSH to log into the ESXi server you don't provide any argument, it automatically uses the key; right?

A. I think it depends on how you have SSH set up but, like I said, in this instance for this session you used your key.

Q. And through your forensic examination I continued to update the ESXi server until I resigned in November, correct?

A. I don't understand. Update?

Q. I mean I continued to administer the server until I resigned, right?

A. You accessed the server until -- I think the server might have been turned off on -- a few days later.

Q. A few days later when?

A. I don't know if it was the 25th. I think the last entry for off.log was from the 18th, I don't think it was -- was used after. The session -- this April 20th session started on the 15th so that's why there is no entries for the 20th in there but I don't believe -- there is not, like, extra logins for the next six or eight months.

Q. No one logged into the ESXi server after April 20th?

A. I would have to review the off log. I don't remember.
Q. Well, you know the ESXi server was continually used after this point, right?
A. When you say "log in", I'm talking about the actual server itself, not logging in through vSphere to make a VM, I am talking about, like, using an SSHT or the root password for the server to log in to the server itself.
Q. Right.
A. Because you said server, administrate the server. For vSphere? I don't know. I don't remember.
Q. Let's jump to slide 81. This e-mail specifically related to the Atlassian projects, correct?
A. I disagree.
Q. You disagree.
A. Yes.
Q. What is the subject of the e-mail?
A. ISB infrastructure permissions transfer.
Q. And what servers were being transferred to ISB?
A. All of the servers running the Atlassian products.
Q. And I was removed from administrating the Atlassian products at this time, right?
A. I believe so from the -- from, like, Crowd. All the keys were removed.
Q. And the ESXi server is not an Atlassian product, correct?
A. It runs the Atlassian products.

Q. It is not an Atlassian product though, right?
A. No. The VM ware of ESXi is not an Atlassian product.
Q. It is a completely different server, right?
A. I wouldn't say completely different. It houses and runs two of the Atlassian servers.
Q. It did until April 25th, right?
A. I believe so.
Q. After that it didn't have any Atlassian products, right?
A. I don't know if those images were still there, but yes, from like a formal perspective, yes, I think they moved them off.
Q. And the ESXi server predated the Atlassian products, correct?
A. I don't remember.
Q. Through your forensic examination you learned that I retained access keys to multiple other servers, right?
A. At this point I only remember the key on the ESX server. I know there were failed logins to the Jira server, to the Stash server.
Q. The Doxygen server; through your examination of the Doxygen server you learned I still had my keys for that, right?
A. I don't remember.
Q. What about the IRC server? Do you remember doing that examination?
A. I do remember doing the IRC server. I don't remember when

or what the status of your keys were for that.

Q. But you were aware up to this point of most of the virtual machines on the server I was administering, correct?

A. I don't know if I can speak to what you were administering or what.

Q. There were at least 20 or so different virtual machines on the ESXi server, right?

A. I believe so.

Q. And your testimony is that you don't recall if I continued to administer them or you don't recall -- is that your testimony?

A. Yeah. I don't recall, like, A, what administrative actions you were performing to, like, the development servers and -- yeah, that's the main -- that's the main part. Like, I was mostly focused on the Atlassian stuff.

Q. And you testified that I was logged into the ESXi server when this e-mail was sent, right?

A. Yes. Your session began on the 15th.

Q. So through your examination you were aware that there were multiple other systems also logged in at this time, right?

A. Can you explain?

Q. I'm sorry. I didn't hear.

A. Can you explain multiple other systems?

Q. Yes. The SSH session into the ESXi server was not the only open session, correct?

A. So it is important to make the distinction of an administrative session to the actual server itself using SSH and what someone might have logged in with vSphere to use a virtual machine. Those are different things.

Q. No, I am talking specifically about SSH.

A. I know that I think it might have been Jeremy's session closed sometime on the 18th. Whether it was before or after this e-mail I'm not sure.

Q. I'm just talking about my open SSH sessions at this time. How many servers were I connected to when this e-mail was sent?

A. I can only speak to the ESXi server.

Q. Retaining your open session to a system is not -- retaining an open session to a system is normal, correct?

A. It depends.

Q. It depends on what?

A. I mean, like, if I had an open session to a machine and then there was a permission change on that exact machine, I think that would be some cause for concern which is why it is included here.

Q. But I don't know, because I -- let me rephrase that question.

Because I used the ESXi key I don't know that permissions -- that the password has been changed, correct?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. If you use an SSH key to log into a server you will not know when a password is changed on the server, correct?
A. Not from doing the normal SSH login process.
Q. OK.
A. It doesn't use the password like that.
Q. Let's take a look at what is in evidence as Government Exhibit 1071. Just the subject of the e-mail.
A. Do you want me to read it?
Q. Just the subject.
A. CMR: Transfer of equipment (especially OSB server) to OSB.
Q. This is a request to transfer ownership of the ESXi server, correct?
MR. DENTON: Objection.
THE COURT: Overruled.
A. I don't know what the formal transfer of investment process was for DevLAN or CIA property in general, but this appears to be you asking what the process is for transferring the OSB server, which I assume is the ESXi server, because it is called OSB, so.
Q. And in the e-mail it's specifically a request to transfer accesses too, right?
A. It just says the equipment and remove your access.
Q. I'm sorry. What was your answer?
A. It says to transfer the equipment and to remove your access.

Q. So it is a request to transfer my accesses, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. And the date of this e-mail?

A. It is April 21st.

Q. But, to your knowledge through the investigation, the ESXi server was never transferred at this time, correct?

A. I don't know. I don't have, like, the property forms from the agency. I don't see how or if a transfer occurred.

Q. I mean, there was no additional keys were added to the authorized key file, right?

A. When we received it I believe your key was the only key that was in there.

Q. I will take that down.

So let's talk a little bit about the ESXi access in general. So you testified earlier I had my key on the ESXi server, correct?

A. Yes.

Q. And that's a root key, correct?

A. Yes. There is only, I think, one account on there.

Q. The primary administrator for the server, correct?

A. Yes.

Q. And what authorization comes with the root server key?

A. I'm not -- can you explain a little further?

Q. What types of commands are root users authorized to

execute?

A. Pretty much everything.

Q. Anything, right?

A. Yes.

Q. By virtue root of server key the user is permitted to perform any command, correct?

A. Yes.

Q. The root key authorizes users to install programs, correct?

A. Yes.

Q. Root key authorizes the user to update the system, correct?

A. Yes.

Q. And root key authorizes the user to delete files, correct?

A. Yes. It will let you do pretty much any kind of administrative action.

Q. So the root user can technically reformat or completely wipe the system, right?

A. Yes, if they chose to do so.

Q. And specifically with respect to virtual machines, the root key authorizes the user to create, modify, delete, snapshot, revert, or do anything at all with virtual machines, right?

A. Yes.

Q. And just for clarification here, the root ESXi key does not grant any privileges on the VMs themselves, right?

A. That's correct.

Q. So you can be a root user of the ESXi server and have no

access to the VMs, correct?
A. Yes. That's correct.
Q. The virtual machines control their own access, correct?
A. They do.
Q. OK. Let's pull up slide 71 in your presentation. Here you note that the root password changed for the Confluence virtual machine, correct?
A. Yes.
Q. And root password is the administrator password, right?
A. Yes, it is.
Q. But there was also a regular user account called Confluence, right?
A. Yes; a service account.
Q. And this regular user account also allowed you to log into the Confluence server, correct?
A. Yes. I don't remember the exact, like, permission string for it. It's an account that is automatically created when you install Confluence. The Confluence service uses it for things, I don't know what exactly.
Q. We can pull up the 1207-11, it is in evidence. So this is the file with both the users, right?
A. Yes.
Q. The Confluence user password was 123ABCDEF, right?
A. I don't remember.
Q. You don't remember the password to the Confluence system?

A. No.
Q. And this password was not changed though, correct?
A. I don't remember. I don't look at the before and after.
Q. We can look at the others. The other one is 1207-21, right?
A. Yes. They look to be the same.
Q. It is the same, right?
A. Yes.
Q. And this password, even though you don't recall it, it would still be reflected in the Confluence, right?
A. Are you talking about in the virtual machine?
Q. No. I mean, there was OSB's ESXi page on Confluence, correct?
A. There was a page, yes.
Q. And it contained the accounts for the -- to log in, correct?
A. I don't remember if it had the -- I don't remember if it had this password. It might have had a password for the, like -- I'm trying to say the password for the user account, for Confluence on disk. It doesn't necessarily have to be the same as the password for the web service, kind of store it in different places. I also don't ever recall seeing the Confluence account ever like logged into like that.
Q. OK. So you don't recall if the user name and password was on the ESXi page? Is that right?

A. ESXi, I don't remember what that password hash resolves to so I don't remember which password that was. I know passwords were stored on that page. I don't know if it is that one specifically.

Q. OK, but you know that I had it saved -- or saved the configuration of that page, correct?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. Through your -- all right, let's pull up what is in evidence as Government Exhibit 1202-3. So this is a save of that server page, correct?

A. Yes.

Q. That contained the configurations for the server, right?

A. Yes, I think that's the page that had the passwords on it, if I remember correctly.

Q. OK. And the Alta backups were mounted on the public/mount directory, correct?

A. That directory does have permissions. It should be owned by root.

Q. The mount directly -- what permissions was it mounted as?

A. I believe it was owned by root. I mean, the share was mounted read/write but that folder on Confluence itself, I believe it to be owned by root.

Q. But it was mounted with read access, right?

A. Yeah, but that doesn't affect the owner. If you are not --

if you logged in as the Confluence user and not the root user, if you tried to access that folder I don't believe you would be able to.

Q. Why?

A. Because of the ownership permissions of that folder.

Q. Well, it doesn't matter who owns it, it matters what is the access controls on the folder, right?

A. The access controls on the folder would be the group that owns it, which I believe was the root group.

Q. I mean, you can set access controls to be -- to have anyone access that?

A. The root user could but not the --

Q. In Linux you can configure access controls through a different directory, right?

A. Yes, you can.

Q. So if you own a directory you can have somebody else access your directory, right?

A. If you change the permissions.

Q. OK. Do you know what the permissions were set to on that directory?

A. I believe it was root root. I believe it was owned by root.

Q. But you don't know for sure what it is sitting here, right?

A. I want to see the exhibit so I can confirm but that's what I remember.

Q. Was there an exhibit that listed the access controls in your slide presentation?

A. Not in the slide presentation, no.

Q. But if the access controls were not set properly, a regular user could log in and access that, correct?

A. Yeah. If the access controls were set to where a user could do that, yes, they could do that.

Q. Next let's go on to slide 87. I just briefly want to touch on this. This was sent on April 20th, correct?

A. Correct.

Q. Can you say whether I even opened or read this e-mail on April 20th?

A. Not sitting here today.

Q. And the e-mail says the migration is going to take place April 25th, correct?

A. That's what the e-mail says.

Q. So from April 20th to 25th there is still five days, right?

A. That's correct.

Q. I think the 20th is a Wednesday, right?

A. This says April 25th is a Monday, so I believe so.

Q. So Thursday, the 21st, Friday, the 22nd, and the weekend, the server is still -- everything is going to be on the ESXi server, right?

A. That's what this says.

Q. Let's take a look at slide 48. So my CIA workstation was

completely intact when you found it, right?

A. Yes.

Q. Which means I did not reformat or wipe it before I left, correct?

A. Not that I could tell.

Q. And have you heard of DBAN?

A. Yes.

Q. DBAN is used to completely wipe a drive, right?

A. Yes, it is.

Q. And it is basic security practice to wipe drives when you finish with them, right?

A. I don't know what CIA's security policy is, but in a general sense if you are finished with a drive that is under your control, yes, you can wipe it.

Q. And through your forensic examination I had multiple copies of DBAN at my desk, right?

A. I believe there were some disks with DBAN. I don't remember if they were found at your desk or not.

(Continued on next page)

BY MR. SCHULTE:

Q. OK. I could have used DBAN to wipe the workstation, right?

A. Yes.

Q. In fact, at the very least, it would have been very easy to zero the unallocated space, right?

A. I don't know about very easy, but that's something you could have done.

Q. I mean the command is just copydevurandom in a file, right?

MR. DENTON: Objection.

THE COURT: Sustained.

(Defendant conferred with standby counsel)

BY MR. SCHULTE:

Q. What is devurandom on Linux?

A. So, there's a -- it's a -- we'll call it a file. If you read it, it will give you a, a random output.

Q. So if you copy that to a file, it will write over unallocated space, right?

A. Yes. It will -- it will store the file, and if there's stuff that was there before, it will get overwritten.

Q. And then you unlink it with the RM command, right?

MR. DENTON: Objection.

THE COURT: Can I see counsel and everybody at sidebar.

(Continued on next page)

(At sidebar)

THE COURT: Part of the reason I took a break is that I think one of the jurors, juror No. 13, has been out cold for at least the last 20 minutes. That, I think, is a metaphor, however, for the cross here, which I just don't get.

What is going on? You elicit from him that it's possible to erase the unallocated space, what program, what command lines. It doesn't matter. No one cares. The jury certainly doesn't understand or get it. You're just wasting their time, my time, and losing the point. So it's not effective for your purposes, and it's just a waste of time.

How much more cross do you have? What do you need to cover?

MR. SCHULTE: I mean I think the point was just the expertise that could be easily -- you know, this could have been easily wiped. I think that's all I was trying to get out. This is just a small --

THE COURT: The particular commands that he might use to do that are not relevant.

MR. SCHULTE: But I mean just showing how small -- you know, if you have to do, like, a long, lengthy process to do it, it's different than running one command, right?

THE COURT: OK. How much more do you have to cover here?

MR. SCHULTE: Want me to go check? I can go check.

THE COURT: No.

MR. SCHULTE: Like, two or three topics left.

THE COURT: OK. Let's move it along. You're losing the jury and not making much progress here. OK? So make it snappy if you can.

Anything that you want to raise or you want to raise?

Mr. Denton.

MR. DENTON: No.

THE COURT: OK. Very good.

(Continued on next page)

(In open court)

BY MR. SCHULTE:

Q. Just briefly -- we'll finish this -- the point is it would only take a few seconds to run these commands, right?

A. Not necessarily.

Q. OK. Let me rephrase that.

It takes a few seconds to type the command, right?

A. Yes.

Q. OK. And if that had happened, there would be no recoverable data from the unallocated space, right?

A. I can't really speak to that. You'd, you'd have to completely fill the disk.

Q. OK. But this was never done, right?

A. I don't recall seeing any evidence of that, no.

Q. OK. Let's turn to slide 83.

There were a ton of commands executed here to attempt to review log files, correct?

A. That's what it appears to be, yes.

Q. And you would agree that this kind of activity is abnormal, right?

A. Abnormal?

Q. Yes.

A. Not this, not this activity. This is just viewing log files.

Q. Well, I guess the breadth, the number of log files and

what's being reviewed is a lot here, right?

A. I would say this is actually pretty minimal. It's only, like, four log files.

Q. All right. You testified on direct that I deleted log files on the ESXi server, correct?

A. Yes.

Q. But none of those log files would have captured copy commands, correct?

A. That's incorrect.

Q. Which one would?

A. Shell.log would capture copy commands.

Q. No. Shell.log is on the ESXi server, right?

A. You didn't specify which server, just copy commands in general.

Q. OK. A copy command from Confluence wouldn't have been logged in those ESXi log files, right?

A. The command itself, no.

Q. The bigger issue is, turning to slide 117, can you tell me what's wrong with what you claim to be deletions here?

A. A lot of deletions.

Q. But the command executed, RM, does not wipe the log, right?

A. It deletes the file.

Q. Well, this command unlinks the file, right?

A. Yes.

Q. OK. There's no slash S argument to RM, right?

A. Well, there's -- no.
Q. And there's no SRM command, right?
A. I -- I don't think SRM was available. I'm actually not even sure dash S is available on -- on ESX or not.
THE COURT: Mr. Leedom, can you translate what those terms mean.
THE WITNESS: Yeah. What Mr. Schulte's describing are flags that you pass to these commands to explicitly, like, overwrite that unallocated space for the file, like, we call a secure erase. I'm not sure what -- I'm not sure if SRM's available on ESX; I don't think it is, and I'm not sure if the S flag or RM either. But no, those flags are not present here.
BY MR. SCHULTE:
Q. OK. But if someone -- if you were attempting to cover your tracks, this is what you would use, right?
A. I disagree. I've seen it just like this plenty of times.
Q. The files themselves are still available, though, right?
A. The content is -- is -- could potentially be there at a later date.
Q. OK. Are you familiar with services?
A. In what way?
Q. Well, in Linux, what's called daemons?
A. Yes.
Q. OK. And ESXi runs daemons for the VMs, right?
A. Yes, I believe there's one that manages the VMs.

MR. SCHULTE: OK. I just want to show the witness what's marked defense exhibit 1204-2 -- sorry, 1204-1.

Q. You're familiar with vSphere, correct?

A. To some extent, yes.

Q. And ESXi, right?

A. Yes.

Q. Were you able to review the contents of any of the log files?

A. Yes.

Q. The content -- I'm sorry -- of the unlinked log files?

A. I don't believe -- I think there was some file side from shell.log, but I don't believe there was any from the others.

Q. OK. And Dave and Jeremy are the ones who came in on April 16, 2016, to take the snapshot of the Confluence VM, correct?

A. Like I said, I don't -- I think Jeremy logged in to the ESXi server.

Q. OK.

A. ISB.

Q. ISB. But neither of them had any experience in Linux or ESXi, right?

A. I do not know.

Q. OK. Can you say whether their actions caused some daemons to crash on that day?

A. I don't recall.

THE COURT: Can we take this document off the screen,

please.

MR. SCHULTE: All right.

Q. Can you say whether or not log files were corrupted on that day?

A. I don't -- I don't remember any -- I can't really speak to the actions they took other than changing the passwords.

Q. OK. But through your knowledge with system administration, if there's a problem with the host service running the VMs, that could cause problems for all the VMs, correct?

A. Depending on how the host service operates and the type of errors, it could potentially. I --

Q. OK.

A. -- kind of have to say as a theoretical, but --

Q. And you don't typically want to restart a service like that because it will restart all the virtual machines, right?

A. It could. I'm not sure exactly of the, like, specific effects of restarting the -- I think the VMware host service, ESXi server.

Q. OK. But at the time you know that there were at least 20 virtual machines on the ESXi server, right?

A. Yes. I don't remember exactly how many were running at the time, but there were multiple machines on there.

Q. OK. So in case of any problems, the best option would be to disable and fix the sole VM causing trouble for the daemon, right?

A. It depends.

MR. SCHULTE: OK. Just going to publish what's your slide 111 here.

Q. Did you notice any pattern at all to your analysis of the log files?

A. Not sure I'm following. Aside from you deleting activity after performing activity?

Q. All right. The core VM 25 technique --

A. I'm sorry?

Q. Did you notice that?

A. I don't know what that is.

Q. OK. So, at 5:55 to 5:57 p.m. was two minutes, right?

A. Yes.

Q. OK. And those are core ESXi system files, right?

A. I'm sorry. But the log files that were deleted between those two minutes?

Q. Yeah.

A. I believe so. I don't know exactly which ones those were, but --

Q. OK. I think we can pull it up.

5:57, those are core ESXi files, right?

A. In the top?

Q. Yeah.

A. Yeah, vmkernel is.

MR. DENTON: I'm sorry, your Honor. Since our screen

isn't working, it would just help if we could identify what we're looking at.

THE COURT: Page 121 of the slide deck.

MR. DENTON: Thank you.

THE COURT: We're trying to get an IT person up to see if he can fix the screens, and here he is.

And could the witness just repeat.

THE WITNESS: Yes. I said vmkernel.log.

THE COURT: And when you refer to core ESXi files, what do you mean by that?

THE WITNESS: So, what I assume it to mean is this would be one of the more important log files that contains, like, an abundance of information about the system.

BY MR. SCHULTE:

Q. OK. And going up to slide 117, this was 5:55, right?

A. Yes.

Q. And these are also core ESXi files, right?

A. Yeah, they're, they're all -- they're all log files for ESXi.

Q. OK. So just going back to slide 111, again, so 5:55 to 5:57 is two minutes, right?

A. Yes.

Q. And then 5:57 to 6:16 is 20 minutes, right, thereabouts?

A. Yes.

Q. 6:16 to 6:38 is 20 minutes, right?

A. 22 minutes.

Q. 6:38 to 6:56 is 20 minutes, right?

A. About.

Q. And then it ends as it began, two minutes, 6:56 to 6:58, right?

A. Yes.

Q. OK. And again, 116, 117 is showing the ESXi files, and then 121 is showing ESXi files, right?

A. Yes.

Q. 122, ESXi files, right?

A. Yes.

Q. And then precisely 20 minutes later, 127, it's another ESXi file, right?

A. Yes.

Q. 129 is -- this is showing the Confluence data stored in the ESXi system, right?

A. Yes, this is the folder where the Confluence virtual machine lives.

Q. OK. So 6:38, this is showing the file in the Confluence directory on the ESXi server, right?

A. Yes.

Q. OK. And then 20 minutes later, on slide 132, some of the same types of files, right?

A. Yes.

Q. 136, again, right?

A. This is back in the, the main ESXi server, log folder?
Q. No. The first command.
A. Rmvmware.log?
Q. Yes.
A. That's in the main log folder for ESXi.
Q. All right. But does the timing, the timing of this and the actions performed indicate to you the core VM 25 technique here?
A. Like I said, I don't know what that is.
Q. OK. Let's go to slide 124. I just want to cover this briefly. Your testimony is that I deleted log files on the ESXi server, right?
A. Yes.
Q. Most of the files are in unique locations on the ESXi server, right?
A. Yes.
Q. And then quoting from your direct, I searched for client logs on the ESXi server, right?
A. Yes.
Q. OK. And were you briefed on my technical training and experience through your investigation?
A. Not, like, explicitly. I knew you were a developer. That's really the extent of it.
MR. SCHULTE: OK. I want to show what's in evidence as Government Exhibit 1114.

Q. And this was just my approved résumé, correct?
A. I can't speak to its approval. This appears to be a résumé with your name on it.
Q. All right. So, from the bottom, I worked at IBM as a system administrator overseeing a test lab with over 900 machines, right?
MR. DENTON: Objection.
THE COURT: Sustained.
Let's move on, Mr. Schulte. Take this down, please.
MR. SCHULTE: OK.
Q. On your final slide you show the eighth floor vaults locked at 7:07, right?
A. I don't remember the exact floor. I don't know if you can pull up the exhibit or not.
Q. OK. I can pull it up.
A. Yes, I believe 8W would be the eighth floor. I believe.
Q. And the CIA maintains surveillance video, correct?
A. I don't know what their, like, physical security retention stuff is.
Q. You were at the building, correct?
MR. DENTON: Objection.
THE COURT: Sustained.
BY MR. SCHULTE:
Q. So through your investigation, you didn't receive any video surveillance from the CIA?

A. I -- I personally did not. I don't know -- like I said, I can't really speak to that.

Q. OK. So, the last thing, just to go through, showing what's in evidence as Government Exhibit 111. And you're familiar with the layout, correct?

A. Very rudimentarily. I've seen this diagram before, but I do not -- I wouldn't be able to tell you, like, who or what was where.

Q. OK.

A. I could say that, yes, this does appear to be the building. That's about as far as I think I can go, unfortunately.

Q. Because you were never on the -- you never went through these eighth or ninth floors?

A. I've been to those floors, but not, like, for any extended period of time or even in any kind of. Like, investigative capacity really.

Q. OK. Just going to show now the badge records, Government Exhibit 105, on page 13, for April 20, and I just want to highlight, this one here is showing an attempted entry at 1745, which is 5:45, on 8W53A, correct?

A. That appears to be the line in the log.

Q. OK. And 8W53A --

(Defendant conferred with standby counsel)

MR. SCHULTE: I think this is a problem with the exhibit.

Does the government have the updated 111, by chance?

MR. DENTON: We do, your Honor.

THE COURT: All right. Why don't we pull that up, please.

Mr. Schulte, Mr. Leedom indicated he's unfamiliar with the particulars of this exhibit, so I'm not sure what you're attempting to do here.

MR. SCHULTE: Yeah, I think just the --

THE COURT: Just ask a question, please.

MR. SCHULTE: OK. If we can zoom in on the left side.

Yeah, if we can zoom in to the numbers there.

Q. So here -- I guess it's hard to see -- do you see in the middle there the 8W53A, right above the -- it says kiosk and to the right is electrical room, 8W75?

A. Is it that door?

Q. Yes. It's up a little bit.

A. It's very hard to read.

MR. SCHULTE: I guess there's no way to zoom in on that.

Q. Do you see it's 8W53A there?

A. I can't -- I see a three. I think that's the best I can really -- I can do, unfortunately.

THE COURT: All right. Let's move on, Mr. Schulte, I think.

MR. SCHULTE: OK. I think this --

THE COURT: It's in evidence. You'll be able to make arguments from it later if you wish, but given that the witness has said he's not familiar with this, I'm not sure there's much more you can do with this here.

MR. SCHULTE: OK.

(Defendant conferred with standby counsel)

MR. SCHULTE: OK. No further questions at this time.

THE COURT: All right.

Redirect.

REDIRECT EXAMINATION

BY MR. DENTON:

Q. Good afternoon, Mr. Leedom.

A. Good afternoon.

Q. This morning, Mr. Leedom, Mr. Schulte asked you some questions about whether material had been deleted from his CIA workstation. Do you remember that?

A. Yes.

Q. And you responded by referring to a host. Do you remember that?

A. That's correct.

Q. What computer were you referring to as the host?

A. That's that E0001, his DevLAN workstation.

Q. And what operating system was that running?

A. Windows.

Q. Was the defendant also running a virtual machine on that

computer?
A. Yes.
Q. Now, Mr. Schulte asked you a number of questions about something he referred to as a transcript file. Do you remember that?
A. Yes, I do.
Q. Did you find any actual transcript files on Mr. Schulte's virtual machine?
A. No.
MR. DENTON: Ms. Cooper, if we could put up Government Exhibit 1703 and go to page 117.
Q. Mr. Leedom, where did you find the files that Mr. Schulte kept calling transcript files?
A. They were all in unallocated space.
Q. Did you draw any conclusions about what happened to those files from the fact that you found them in unallocated space?
A. They'd been deleted.
Q. Now, Mr. Schulte also asked you a series of questions about whether you found a copy command in these files. Do you remember that?
A. Yes.
Q. And in particular, a copy command with respect to the Altabackups files, do you remember being asked those questions?
A. Yes.
Q. Where are the commands that we've been looking at that

Mr. Schulte showed you being run?
A. Like what's on this slide right now?
Q. Yes.
A. So, these commands are all being run on the ESXi server.
Q. Did the ESXi server have access to the Altabackups directly?
A. No.
Q. Would you need access to the Altabackups directly to be able to copy files from them?
A. Yes.
Q. Where were the Altabackups mounted directly?
A. To the Confluence VM.
Q. Did you find any log of the defendant running a copy command in the Confluence VM to copy the Altabackup files?
A. No.
Q. Why not?
A. We couldn't, because any log files from that VM were deleted after the reversion.
Q. And why were they deleted after the reversion?
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. Because once you do that reversion, everything that -- anything that would have been typed into that machine during that time period would get erased.
Q. Let's talk a little bit about snapshots and reversions for

a moment, Mr. Leedom.

MR. DENTON: Ms. Cooper, could we go to page 68 of Government Exhibit 1703.

Thank you.

Q. Mr. Leedom, Mr. Schulte asked you some questions about whether you learned that snapshots and reversions were commonplace. Do you remember that?

A. Yes.

Q. How many snapshots were taken of the Confluence virtual machine?

A. Three, just like here.

Q. Is that the total number that were taken?

A. No.

Q. How many were taken?

A. Four, in total.

Q. What happened to the third one?

A. It was deleted.

Q. By whom?

A. Mr. Schulte.

Q. Mr. Schulte also asked you some questions about SSH keys just a moment ago. Do you remember that?

A. Yes.

Q. He asked you what SSH keys authorize?

A. Yes.

Q. Whether they authorize making changes to virtual machines,

right?
A. Yes.
Q. What do you mean when you say it authorizes that?
A. So, when you store an SSH key, it's associated with a, like, a certain user account; in this case, the administrator user.
Q. On April 20, 2016, did the CIA allow Mr. Schulte to make changes to the Confluence virtual machine?
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. When you say allow, do you mean did he have permission to, or --
Q. Is there a distinction in this context between having permission and being authorized through an SSH key?
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. So, if your, if your key is there, then you can, you know, physically log in to it and make changes. The only thing stopping you would be if your key wasn't there.
Q. Is that different from being authorized to by policy?
A. Yes.
Q. Now, Mr. Schulte asked you a number of questions about hypothetical possibilities with respect to the DevLAN system, right?
A. Yes.

Q. As a general matter, what level of permissions were required to access the Atlassian backups?

A. You'd need administrator permissions.

Q. Now, with respect to some of those hypotheticals, Mr. Schulte asked you about foreign adversary penetrations of DevLAN. Do you remember that?

A. Yes.

Q. Was that a focus for you when you began your investigation?

A. It was.

Q. Was that something that you looked for evidence of?

A. Yes.

Q. Did you find any evidence of that?

A. No.

Q. Mr. Schulte asked you some hypothetical questions about things that Dave and Jeremy might have done. Do you remember that?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. Yes.

Q. Were Dave and Jeremy also administrators of the system?

A. Yes, they were.

Q. As part of your investigation, did you focus on whether administrators other than Mr. Schulte might have taken this data?

A. Yes.

Q. Did you include Dave and Jeremy in that?
A. Yes.
Q. Did you find any evidence that they had done that?
A. No.
Q. With respect to the other hypotheticals that Mr. Schulte asked you, when --
MR. SCHULTE: Objection to characterization.
THE COURT: Overruled.
BY MR. DENTON:
Q. Did you find any evidence of these theoretical possibilities?
A. No.
Q. He also asked you at various points to focus on single pieces of your analysis. Do you remember that?
A. Yes.
Q. When conducting forensic analysis, do you focus on single items of evidence in isolation?
A. It's about the whole picture.
Q. Why is that?
A. Just about anything taken in isolation, out of context, is -- it's not going to provide the necessary information to understand it.
Q. So let's take an example of that.
MR. DENTON: Ms. Cooper, if we could go back to page 117 of Government Exhibit 1703.

Q. Do you remember Mr. Schulte asked you some questions about what constituted normal system administrator activity?
A. Yes.
Q. Taken in context, is what is shown in Government Exhibit 1203-29 normal system administrator activity?
A. No.
Q. Why not?
A. Because the amount of logs and type of logs that are being deleted here, you -- you just wouldn't do it.
Q. In your experience, what is it consistent with?
A. Activity of trying to --
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. Activity of trying to cover your tracks, trying to, trying to, you know, clean up after yourself, trying to inhibit others' ability to see what happened at the time these log files stored information.
MR. DENTON: If we could go to page 139, Ms. Cooper.
Q. And Mr. Schulte also asked you some questions about whether using snapshots and reversions was normal system administrator activity. Do you remember that?
A. Yes.
Q. Was the pattern of reversions and snapshots by Mr. Schulte on April 20 consistent with normal administrator activity?
A. No.

Q. How was it inconsistent with that?
A. I mean we can even just look at the Confluence VM. There were four snapshots taken over the course of a couple years. And this had never happened before, this snapshot reversion for this, especially within, like, a one-hour time frame. It's not something that -- you know, it's not something that happened every Friday at 1:00. This is an instance, a single instance of something outside the normal.
MR. DENTON: And then we could go to the next page, page 140.
Q. What was outside the normal about Government Exhibits 1207-27 and 1207-30?
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. All these access times are the same and almost identical to the date created and date modified. For these two entries that are highlighted, for the March 3 backup, the access time is different. It's on April 20.
Q. And is that a fact that you considered together with other parts of the forensic evidence that you found in this case?
A. Absolutely.
Q. And did that lead to the conclusions that you drew?
A. Yes.
Q. What conclusion was that?
A. That the defendant copied these backup files while the

Confluence VM was in that reverted state.

Q. And as a result of the defendant's activities, were you able to recover the specific command to copy those files?

A. No.

MR. DENTON: No further questions, your Honor.

THE COURT: Any brief recross?

RECROSS EXAMINATION

BY MR. SCHULTE:

Q. Mr. Denton asked you about the level of permission needed to access the Altabackups, correct?

A. Yes.

Q. But the access controls were lost before you were able to recover them, correct?

A. To some extent they were, yes.

Q. I mean you never recovered any access controls for the Altabackup, correct?

A. I think we had to, like, for the folder, like, you had to be root to access the folder. But all of the allow listing, IP address information for the config, we didn't have that.

Q. OK. So sitting here today, you don't know what the permissions on those allow and deny lists were, correct?

A. Correct.

Q. Mr. Denton asked you whether you investigated Dave and Jeremy, correct?

A. Yes.

Q. And just to confirm, Dave C. saved a copy of Stash on his home directory, correct?

A. Yes. We looked at it.

Q. And his home directory was public, correct?

A. I don't know the, the permissions for that home directory. I -- I think from previous statements from Dave, he said that it had -- he had, like, locked it down. But I don't remember exactly what the -- what the permissions are exactly. But I just know in some previous statements I think that that's what he'd said.

Q. Well, we saw defense exhibit 1201 earlier and it doesn't show any access list controls directory on that, right?

A. I think that was just for the, like, root directories. I don't think that list showed every single person's home folder. Because you could change the permissions on your home folder even though the people could see, like -- like, they could even see your folder but may not be able to go into your folder based on the permissions.

Q. But those permissions would have been logged in the exhibit, right, for all the access controls?

A. I don't know how large that, that exhibit was that we looked at. That may have just been an exhibit of, like, the top-level shares.

Q. So your testimony is that you don't know what access his home directory was set to?

A. Sitting here today, I don't -- I don't recall the exact permissions. I just know -- I think hearing from Dave that they were -- they were changed. And I'm sure I reviewed them at some point in the past, but I don't remember exactly right now.

Q. OK. But Dave C. is the same individual who lost the hard drive with Stash on it too, right?

MR. DENTON: Objection.

THE COURT: Sustained.

Next line, please.

BY MR. SCHULTE:

Q. OK. And you said the snapshot reversion was outside the normal, correct?

A. Yes.

Q. But it happened at 5:35 p.m. on a weekday, correct?

A. I believe so.

Q. And people were still working, correct?

THE COURT: All right. Sustained. Asked and answered.

Any new questions based on the redirect, Mr. Schulte?

BY MR. SCHULTE:

Q. The transcript files you talked about with Mr. Denton, about the log-in or copy command, but if a log-in to the VM or copy command had been run, you would have seen that in the transcript files, correct?

A. It really depends.
Q. Depends on what?
A. Well, A, if those are even actually transcript files, and B, like, if all of the -- if they were there, if -- if that activity was even stored in one was available. I mean all I can speak to is the available evidence, and there was nothing in there showing that.
Q. OK. But those transcript files are from my CIA workstation, correct?
A. Yes.
Q. And they're showing log-in -- they're showing commands being run on a remote server, correct?
A. Yes.

MR. SCHULTE: OK. No further questions.

THE COURT: All right. Can we let Mr. Leedom go?

MR. DENTON: We can, your Honor.

THE COURT: All right. Mr. Leedom, you may put your mask back on and step down. You're excused.

(Witness excused)

THE COURT: Mr. Denton, next witness.

MR. LOCKARD: The government calls Michael Berger.

MICHAEL BERGER,

called as a witness by the government,

having been duly sworn, testified as follows:

THE COURT: You may proceed, Mr. Lockard.

MR. LOCKARD: Thank you, your Honor.

DIRECT EXAMINATION

BY MR. LOCKARD:

Q. Good afternoon, Mr. Berger.

A. Good afternoon.

Q. Who is your employer?

A. I work for the Federal Bureau of Investigation.

Q. And what is your position with the FBI?

A. I'm a computer scientist, currently assigned to the New York field office.

Q. For how long have you been a computer scientist with the FBI?

A. Approximately ten years.

Q. Do you have any degrees relating to computer science?

A. Yes, I do.

Q. And what degrees are those?

A. I have a bachelor's of science in computer science, I have a master's of science in computer forensics, and a master's of science in computer science.

Q. You said you have a master's in computer forensics?

A. That is correct.

Q. What is computer forensics?

A. Computer forensics is the area of study that deals with applying forensic science to looking through digital evidence.

Q. Do you have any other professional responsibilities

relating to the field of computer science?
A. Yes, I do.
Q. And what is that?
A. I also teach digital forensics.
Q. And where do you teach?
A. At the school of engineering at New York University.
Q. For how long have you taught digital forensics at NYU?
A. About three years.
Q. And we talked about computer forensics. What is digital forensics?
A. Digital forensics is just the more modern term for computer forensics. You can think of it as the overarching term that would include computer forensics, network forensics, mobile device forensics, things like that.
Q. Turning back to your responsibilities as an FBI computer scientist, are you currently assigned to any particular group within the FBI?
A. Yes, I am.
Q. What group are you assigned to?
A. I'm assigned to the cyber branch of the New York field office, specifically cyber squad CY1.
Q. What types of cases does the branch that you're assigned to generally investigate?
A. Cyber branch generally investigates what are known as computer intrusions, basically a fancy way of saying hacking,

someone getting unauthorized access to a computer that does not belong to them.

Q. And your squad in particular, does it investigate a particular type of cyber crimes?

A. Yes.

Q. What do you typically investigate?

A. Complex national security-based intrusions.

Q. Have you participated in professional training related to computer science and computer forensics?

A. Yes.

Q. And what types of trainings have you participated in?

A. I've taken both trainings internal to the FBI as well as external vendor-provided trainings.

Q. Have you provided professional training to others?

A. Yes.

Q. Can you describe what type of professional training you've provided to others?

A. Within the FBI I've provided internal trainings to groups of people or sometimes my squad or sometimes the entire cyber branch.

Q. Mr. Berger, are you familiar with the FBI's CAT team?

A. Yes, I am.

Q. And what is the CAT team?

A. It's the cyber action team.

Q. And I think we heard a little bit about that from

Mr. Leedom's testimony. What kind of work does the CAT team do?

A. So, the CAT team is the FBI's headquarters-based incident response team. They can respond both domestically and internationally to very significant cyber intrusion incidents or any other investigations that have a high level of technical complexity.

Q. And do you have a role with the CAT team?

A. I do.

Q. What is your role?

A. I'm a member of the team.

Q. For how long have you been a member of the CAT team?

A. About six years.

Q. Have you participated, in your career as an FBI computer scientist and a member of the CAT team, in investigations of computer hacking?

A. Yes.

Q. Have you participated in investigations of insider threats?

A. Yes.

Q. In your investigations, have you applied any kind of specialized analyses?

A. Yes, I have.

Q. What kinds of specialized analyses have you applied in those investigations?

A. I've conducted traditional disk forensics, looking at

forensic images on hard drives from computers. I've also conducted memory analysis, where the contents of volatile computer memory is captured and then analyzed. I've analyzed log files. I've reverse engineered malware, things along those lines.

Q. And Mr. Berger, have you been qualified as an expert in court proceedings in the past?

A. Yes, I have.

MR. LOCKARD: Your Honor, the government offers FBI Computer Scientist Michael Berger as an expert in the subject of computer science, computer forensics, and digital forensics.

THE COURT: Any objection?

MR. SCHULTE: No objection.

THE COURT: All right. Received.

Ladies and gentlemen, you'll recall my instructions a few days ago about what an expert witness is and may testify to. Those instructions govern here, and as I told you, I'll give you additional instructions on that score at the conclusion of the case.

Mr. Lockard, you may proceed.

MR. LOCKARD: Thank you, your Honor.

Q. Are you familiar with an investigation relating to the WikiLeaks Vault 7 release?

A. Yes, I am.

Q. When did you first become involved in that investigation?

A. Approximately the middle of March 2017.

Q. And approximately how long after the first of the Vault 7 releases was that?

A. I believe it was about one or two weeks.

Q. And broadly speaking, what was your role in the investigation?

A. My role was to provide digital forensics assistance with some of the evidence that was recovered at the defendant's apartment.

Q. And what other roles did you play in the investigation as time went on?

A. Throughout the investigation, I also performed analysis on some of the data that was disclosed by WikiLeaks in comparing it to data that was retained by the CIA in their internal systems.

Q. Broadly speaking again, what types of digital evidence did you review in your role in the investigation?

A. So, I reviewed information provided by the CIA from the DevLAN system interpreting the form of database backup files. I reviewed disk images that were obtained from the defendant's apartment. I also looked at data provided by service providers pertaining to the defendant's actions.

Q. In your work as an FBI computer scientist, have you used a computer user's online activities or computer activities as part of your investigation?

A. Yes.
Q. And how does the user's activity inform your forensic analysis and conclusions?
A. Depending on what those activities were, they may show an indication of different types of techniques that the person might have been researching or looking up, and those would correlate to possibly evidence of those techniques being found on the evidence provided.
Q. Did your review and analysis of the categories of evidence that you describe include the application of some of the specialized analytical techniques that you described earlier?
A. Yes.
Q. So, Mr. Berger, do you have in front of you a binder with Government Exhibit 1704 inside of it?
MR. LOCKARD: Ms. Cooper, if we could show Mr. Berger the first page of Government Exhibit 1704.
Q. Mr. Berger, are you familiar with what's shown here?
A. Yes, I am.
Q. Did you participate in its preparation?
A. Yes.
Q. Would referring to Government Exhibit 1704 assist you in explaining your methodology, some of the relevant evidence, and the conclusions that you drew?
A. Yes.
MR. LOCKARD: Your Honor, we would request permission

to publish 1704 as a demonstrative exhibit.

THE COURT: Any objection?

MR. SCHULTE: Yes. Same objection to the other one.

THE COURT: All right. Overruled.

You may display it.

Ladies and gentlemen, again, for the moment at least, this is not being admitted into evidence. It's just a demonstrative, an aid to allow you to help understand the witness's testimony. It's the witness's testimony, unless and until this is admitted as an exhibit, it is only the witness's testimony that is the evidence.

You may proceed.

MR. LOCKARD: Thank you, your Honor.

Q. Mr. Berger, are you familiar with the organization known as WikiLeaks?

A. Yes, I am.

Q. I'd like to turn to page 54 of your presentation. In the course of your investigation, have you reviewed the WikiLeaks site?

A. Yes, I have.

MR. SCHULTE: Objection.

THE COURT: Overruled.

MR. LOCKARD: Could we turn to the next page, please, 55.

Q. And does this display a portion of the WikiLeaks website?

A. Yes, it does.

MR. LOCKARD: Could we turn to page 56, please.

Q. What's shown here?

A. This is a screenshot of the portion of the WikiLeaks website that specifically details how to submit content to WikiLeaks.

Q. And during what time period was this particular version of the WikiLeaks website available?

A. This was made available on WikiLeaks' website on April 23 of 2016.

THE WITNESS: Can we turn to page 57, please.

Q. What's shown here in the URL of this version of the WikiLeaks site?

A. So, in the URL, you can see that the WikiLeaks.org website could access from archival copy created on 2016 -- April 23 of 2016, and it was accessed by the site in the beginning, web.archive.org, also commonly referred to as the Wayback Machine.

Q. And is the Wayback Machine a resource that you have used in the course of your investigations as a computer scientist?

A. Yes.

Q. And is it a resource that's been used more generally in cyber investigations at the FBI?

A. Yes.

MR. LOCKARD: If we could turn to page 58.

Q. So in this version of the WikiLeaks website available in April of 2016, did WikiLeaks provide any instructions or advice to potential leakers?

A. Yes.

MR. SCHULTE: Objection.

THE COURT: Overruled.

BY MR. LOCKARD:

Q. What instructions did WikiLeaks provide?

A. So, they list several pieces of information on this site. As depicted in the screenshot here, they also recommend the use of two different utilities, TOR and Tails.

MR. LOCKARD: And we can move to slide 59.

Q. Is that what's described in this portion of the website?

A. Yes.

MR. LOCKARD: Move to slide 60.

Q. Mr. Berger what did WikiLeaks say about the TOR service?

A. They describe TOR as an encrypted anonymizing network that makes it hard to intercept communications.

Q. Are you familiar with the TOR network?

A. Yes, I am.

MR. LOCKARD: Turn to page 61, please.

Q. Can you describe what is TOR and how does it work?

A. So, TOR is set up as kind of how it was just described, an encrypted anonymizing network. There are many people out there that run what are called TOR nodes. They set their computer up

as a TOR node, and it connects into TOR network.

If a user, in this case shown on the demonstration slide, Alice, wants to use the TOR network, she would use the TOR client on her computer that would connect through the TOR network. The TOR network would then establish a circuit through the TOR network going between several different TOR nodes until eventually it would emerge from what we see referred to as a TOR exit node, and Alice's traffic would then emerge onto what we know as the regular internet.

If at any point anyone looked at any of the communications between Alice and the first TOR node or between any of the other TOR nodes, they would not be able to identify any discerning information or see the content of that data being transferred.

MR. LOCKARD: Ms. Cooper, can we please turn to page 74.

Q. Mr. Berger, in your role in the investigation, did you find evidence of the defendant's use of TOR?

A. Yes.

Q. What are we looking at on page 74, displaying Government Exhibit 1401-12?

A. This is a screenshot from a Linux virtual machine that was found on the desktop computer in the defendant's apartment.

Q. So, we've heard a little bit about virtual machines in the course of the trial testimony, but could you please just

summarize -- again, very briefly -- what is a virtual machine?
A. So, a virtual machine is essentially a way to run one or more additional computer systems within a physical computer system. It allows for running different operating systems. For an example, you could have a Windows computer and you want to run a Linux system without actually getting a second, additional computer.
Q. And when a user is running a virtual machine on their desktop, are they able to switch back and forth between the virtual machine and other applications?
A. Yes.
Q. Are you able to run more than one virtual machine at a time?
A. Yes.
Q. What's shown here in the circled icon on the defendant's virtual machine desktop?
A. That is the icon for the TOR browser.
MR. LOCKARD: Ms. Cooper, if we could please turn back to page 62.
Q. So, looking again at the version of the WikiLeaks website available in April of 2016, what did WikiLeaks say about a service called Tails?
A. WikiLeaks instructs that if you are at high risk and you have the capacity to do so, that you can also access the submission system through Tails.

Q. Now, through your work, had you become familiar with the Tails system?

A. Yes.

Q. And generally speaking, what is the Tails system?

A. Tails is a, what is referred to as a live operating system; that is, it is used without being installed to your computer. It is commonly placed on either a DVD or a flash drive. You would put that into your computer, and your computer would boot off of that device. It's a live system in that everything that is happening in the operating system exists in what we refer to as volatile memory; that is, nothing is saved past the power cycle of the computer. And the operating system doesn't actually save anything to your hard drive unless you intentionally do so.

Q. And from the viewpoint of a digital forensics investigator, what is the effect of someone using Tails on your ability to recover evidence of their activities?

A. It makes it very, very difficult.

MR. LOCKARD: If we could turn to page 63.

Q. Mr. Berger, what's shown here?

A. This is the website where you would go to find information about and download Tails.

Q. And is this version also obtained from that web archiving service, the Wayback Machine?

A. Yes, it is.

Q. And during what time period was this version of the Tails website available?

A. This was made available on April 22 of 2016.

MR. LOCKARD: And if we can turn to page 64.

Q. So Tails has a description of the live operating system that you just described. What does Tails say itself about the purpose and use of the Tails system?

A. It talks about how it aims at preserving your privacy and anonymity. It also allows you to use the internet anonymously and circumvent censorship. It mentions how it leaves no trace on the computer unless you were using it -- unless you ask it to explicitly.

Q. What is the relationship between Tails and the TOR network?

A. So, the way Tails works --

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. The way Tails works is that once it's booted up and ready for use, it automatically connects to the TOR network and funnels anything you do in the Tails operating system over the TOR network.

MR. LOCKARD: If we can move to slide 65.

Q. What version of Tails was available in April of 2016?

A. That would be version 2.2.1.

Q. Now, Mr. Berger, in your review of the defendant's computing equipment, did you find evidence of the Tails

program?

A. Yes.

MR. LOCKARD: Could we turn to slide 72, please.

Q. Mr. Berger, what's shown here in this slide from Government Exhibit 1403-7?

A. This is a forensic artifact detailing details and metadata about the file tails-i386-2.2.1.torrent.

Q. What is the significances of the dot-torrent part of that file name?

A. So, that indicates this was a Torrent file used to obtain files and share files over a Torrent network.

Q. And what is the Torrent network?

A. The Torrent network is a system designed to allow users to both download files and share files they already have. When you obtain a Torrent file; that is, information about the file you wish to obtain, specifically what other nodes on the Torrent network would have that file that you can get the content from. The Torrent protocol allows you to download bits and pieces of the file you want from multiple people at once.

Q. So, there's various pieces of information listed here about that Tails-Torrent file. Were you able to conclude when this file was downloaded?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. Yes.

Q. And what did you conclude?
A. I concluded it was downloaded on April 24, 2016, at 5:02 p.m. local time.
Q. And is that the time and date that's listed next to the "last written" field?
A. That's correct.
Q. Now, there's some other date fields included here in this exhibit, specifically drawing your attention to the date of May 10 for "last accessed" and "file created." Were you able to draw any conclusions about the significance of those later dates on May 10?
A. Yes.
Q. What conclusions were you able to draw?
A. I was able to draw the conclusion that this file had been moved at that point in time from one drive to another.
Q. And how would that affect the "last accessed" and file-created date while still remaining -- preserving the last-written date?
A. Generally, when a file is moved between two different drives or two different file systems, the last written -- or also referred to as last-modified date -- is usually preserved. However, because the file is now being re-created on a new file system, most often the created and access times are created as of new during that operation.

(Continued on next page)

BY MR. LOCKARD: (Continuing)

Q. Now looking at the file name, Tails-I 386-2.2.1, what was the version of tails that was available as of April 2016?

A. 2.2.1.

Q. Now, Mr.Berger, in your review of the defendant's home computing equipment, did you find a copy or a forensic artifact relating to the Tails program itself?

A. No, I did not.

Q. Were you able to reach any conclusions about why you did not find the Tails program?

A. Yes.

MR. SCHULTE: Objection.

THE COURT: Overruled.

Q. And what conclusions were you able to draw?

A. It was no longer available due to the computer drives being formated at a later date.

Q. So you mentioned reformatting. Did your review of the defendant's home computer equipment identify evidence relating to data deletion and data destruction?

A. Yes, it did.

Q. If we could turn to page 82 of this slide, please? Now, before we talk about that evidence, perhaps you could describe for us some of the principles behind data deletion, and in particular could you please describe what happens in an ordinary delete command to delete a file?

A. Sure. So the way files are stored on a hard drive it can be thought of as, essentially, a table of contents. There is a listing of files in the beginning of the hard drive and they have locations or addresses of where the actual content for those files are stored on the hard drive. In the diagram indicated here, we can see a box where it says File System. That is essentially that table of contents, it is a listing of files, and those files are labeled as active meaning they're active, they're current, they have not been deleted. Each of those files points to a location on the actual hard drive where the data for the corresponding file is stored.

Q. And can you just describe how that explanation you just gave of the file system is displayed in this representation here on slide 82?

A. Yes. So you can see how the file system in that box has a listing. That, essentially, is the table of contents that is going to list the files and it is also going to store additional metadata about each files. The cylinder on the right represents the main portion of the hard drive where the actual content of files is stored.

Q. If we can move to slide 83, does this show what happens in an ordinary deletion command?

A. Correct.

So in an ordinary deletion command the file is marked as deleted in the file system and it no longer points to the data.

However, the data for the underlying file in this example, file 3, the data is still there.

Q. Are you familiar with the phrase or the term "unallocated space"?

A. Yes, I am.

Q. How does that term relate to the concept you just described?

A. So if file 3 was deleted through a standard delete, the address where the file 3 data is located would no longer be considered allocated, it would be considered part of unallocated space, that is space on the hard drive that is not currently allocated to an active file and is available for reuse by the file system.

Q. And is file data that has been deleted through an ordinary delete command but remains in unallocated space, can that be recovered through forensic analytical techniques?

A. It can be.

Q. Are there methods to delete files that does not leave any forensic evidence behind?

A. Yes.

MR. LOCKARD: Can we turn to page 83? I'm sorry. 84. Thank you.

Q. Mr. Berger, can you describe how a secure file deletion utility would work?

A. In order to securely delete the file, the entire area where

the data file exists needs to be written over with what additional data. In this slide the example is showing how the content of file 3 has been overwritten with all zeros and the actual entry for file 3 has been removed from the file system.

Q. Through your work as an FBI computer scientist, have you become familiar with examples of these types of programs that securely delete particular files?

A. Yes.

Q. What's an example of a utility like that?

A. One such program would be Eraser Portable.

Q. In your review of the defendant's home computer equipment, did you find evidence of the use of Eraser Portable?

A. Yes.

MR. LOCKARD: Ms. Cooper, can we turn to page 88, please?

Q. Mr. Berger, can you describe what is shown here?

A. So this is a screenshot from a forensic program showing the file system of a thumb drive or flash drive that was recovered from the defendant's apartment.

Q. And this is derived from Government Exhibit 1404-1?

A. Yes.

Q. And what folder are we looking at on the right-hand side?

A. Specifically we are looking at the Eraser Portable/data/settings subfolder.

Q. And what type of information is stored in the settings

folder?

A. Configuration information for the program, as well as file artifacts from the use of the program.

Q. Did you review the contents of these files?

A. Yes, I did.

Q. Let's look at slide 89. And what is shown here in this slide which is derived from Government Exhibit 1404-15?

A. This is what is called the schedlog.text, which is a log file where Eraser Portable logs certain activities.

Q. And focusing in on the entries that are highlighted in red on -- or I'm sorry, on April 23rd of 2016 and April 28th of 2016, what type of activity is reflected there?

A. On April 23rd, 2016, at 6:12 p.m., it indicates that the Eraser Portable program started. On April 28, 2016, at 8:36 p.m., it indicates that the Eraser Portable program was closed.

Q. From your review of this thumb drive, were you able to identify what type of activity occurred between April 23rd and April 28th of 2016?

A. Yes.

Q. Can we turn to slide 90, please?

So, Mr. Berger, can you sort of describe generally what is shown on this slide which is from Government Exhibit 1404-2 and how were you able to use it in your forensic analysis?

A. So this is, again, from a forensic program showing the

contents of the Eraser Portable app folder on that thumb drive including recovered deleted files. Specifically, the file default.ERS indicated here _efault.ERS, and you can say varying in size and varying last written dates. This was a file that our analysis concluded stores files that are added to Eraser Portable to be queued for deletion.

MR. LOCKARD: If we can turn to slide 91?

Q. Are we now looking at the contents of one of those versions of that default.ERS file?

A. Yes.

Q. And what is the date of this version of that file?

A. So this file was last modified on April 23rd, 2016, at 6:20 p.m.

Q. And what is reflected in the contents of that file?

A. There are two folders that are listed there that were scheduled for deletion.

Q. And what is the first folder of files that was scheduled for deletion on April 23rd?

A. The inner most sub folder is entitled Brutal Kangaroo.

Q. Have you become familiar with Brutal Kangaroo?

A. Yes, I have.

Q. And what is your understanding of what Brutal Kangaroo is?

A. It was a program the defendant worked on while he was a developer at the CIA.

Q. And according to the file path information for Brutal

Kangaroo, where was the data that was scheduled to be deleted, where was it stored at the time?

A. It was stored in a series of subfolders that were located on the D drive on the defendant's computer.

Q. And can you give us just a brief overview of how the defendant's home computer was set up?

A. So the defendant had two different drive volumes, the C drive and D drive. The C drive is where the operating system was installed and that was a single hard drive. The D drive was where lots of additional data was stored and that was what is called a RAID volume, specifically RAID 5. That means there were three hard drives connected together through a RAID controller. The RAID controller combines the available space on those three drives and also allows for redundancy in case one of those drives fails and presents as a single volume to the computer.

Q. Now, does this file reflect the contents of the Brutal Kangaroo folder?

A. It does not.

Q. Were you able to identify through your review of the defendant's home computer equipment what the contents of that folder were?

A. I was not.

Q. And why not?

A. That folder was securely deleted through the use of Eraser

Portable.

Q. And then there is also a second folder that is listed here?

A. Yes.

Q. And what is the name of that folder?

A. Array list.

Q. And do you know what the contents of that folder were?

A. I do not.

Q. Were you able to recover any of those files from your review of the defendant's computer?

A. I was not.

MR. LOCKARD: Can we turn to the next slide, 92?

Q. So, Mr. Berger, what version of that queue file are we looking at here in this slide?

A. It is the version that was last modified on April 28, 2016, at 8:36:36 p.m.

Q. And what is listed in the queue file for Eraser Portable as of April 28th of 2016?

A. There are five different files named data.bkp through data6.bkp.

Q. Were you able to reach any conclusions about what happened with these inside the Eraser Portable program?

A. Yes.

Q. And what were you able to conclude?

A. They were added to the queue to be deleted, however the programs closed before they were securely deleted.

Q. And how were you able to determine that?
A. Through extensive testing of the Eraser Portable program and determining what types of artifacts it leaves on a drive under what circumstances and essentially able to recreate the timeline of deleted files we found on the thumb drive.
Q. Now, from the file path information for these five .bkp files, where were those files stored at the time they were in this deletion queue?
A. They were stored in subfolders that were located on the D drive.
Q. So, Mr. Berger, you said that the Eraser Portable program was closed without deleting these five .bkp files?
A. That's correct.
Q. In your review of the defendant's home computer equipment, did you identify these files or forensic artifacts of these files?
A. I did not.
Q. And were you able to reach any conclusions about why not?
A. Yes.
Q. What conclusions did you reach?
A. The D drive was securely wiped.
Q. Now, from your review of the defendant's home computer equipment, are you familiar with this naming convention of data.bkp?
A. I am.

Q. Did you find other files on the defendant's computer with that naming convention?
A. I did.
Q. Did any of those files remain when you reviewed the home computer equipment?
A. Yes.
Q. But not these five?
A. Correct.
Q. So, Mr. Berger, we have been talking about the secured deletion of particular files or folders. Are you also familiar with methods of deleting data on entire drives?
A. Yes.
MR. LOCKARD: Ms. Cooper, if we could please turn to slide 82 again?
Q. So this is that representation of the file system and how it keeps track of where data associated with particular files lives?
A. Correct.
Q. Are you familiar with the concept of formatting a drive?
A. I am.
MR. LOCKARD: If we can turn to page 85?
Q. How does formatting a drive work?
A. So formatting essentially recreates the file system or what we talked about earlier is the table of contents, it essentially wipes out the table of contents, creates a new

blank slate in its place and says, OK, the drive is ready for new files. It does not do anything to the underlying data of those files. So as I indicated in the screenshot or the diagram here, the file system is empty, it doesn't have any files that it knows about or the content of the previous files that existed are still present on the drive.

Q. And after a format of a drive like the type you just described, is that file data potentially available for recovery by a forensic examiner?

A. Yes.

Q. Are there ways of deleting a hard drive that do not leave forensic artifacts behind?

A. There are.

MR. LOCKARD: If we can turn to page 86?

Q. Can you describe how that type of disk wiping works?

A. So similar as to how I mentioned earlier, a secure file deletion utility would work zeroing out the content of a particular file, a utility to securely wipe the entire drive would overwrite all of the area on the drive. In this case it is shown in the diagram as the entire area showing the file system or the table of contents has been zeroed out as well as all of the underlying data for the files on that drive have also been zeroed out. Essentially, the program would go through every available slot on that drive that could store data and overwrite it with a zero or, possibly, random data.

Q. So, Mr. Berger, what are some of the reasons why an ordinary computer user might format or reformat their hard drive?

MR. SCHULTE: Objection.

THE COURT: Overruled.

A. Reformatting is commonly done if a user decides to possibly change the operating system they are using on the computer, or if it has gotten a little slow over the years and they want to re-install the operating system and start fresh.

Q. Is a secure disk wipe necessary in order to achieve those purposes?

A. It is not.

Q. Now, Mr. Berger, you have been present through the testimony of some of the other witnesses at this trial; is that right?

A. That's correct.

Q. And did you hear some questioning earlier today about a program called Darik's Boot and Nuke?

A. I did.

Q. In your review of the defendant's home computer equipment, did you find evidence relating to Darik's Boot and Nuke?

A. Yes, I did.

MR. LOCKARD: Ms. Cooper, can we please turn to page 95?

Q. So looking here at this slide which is derived from

Government Exhibit 1402-8, Mr. Berger, can you describe what we are looking at?

A. So this is, again, a forensic artifact showing details of metadata about a particular file. The file is entitled DBAN-2.3.0 _I586.I S O.

Q. And were you able to reach any conclusions about when this file was downloaded?

A. Yes.

Q. And what did you conclude?

A. It was downloaded on April 30th, 2016, at 11:28 a.m. local time.

MR. LOCKARD: If we can turn to page 96?

Q. Is that the date that is highlighted here in the last written field?

A. Correct.

Q. And again, I think as we saw with that Tails torrent file there is later dates reflected in the last accessed and filed created fields of May 5th, 2016. Were you able to reach any conclusions about those later dates in those fields?

A. Again, that indicated that the file had been moved between hard drives.

Q. Mr. Berger, did you do anything else with this DBAN file that was found on the defendant's home computer?

A. I did.

Q. What did you do?

A. I copied it out of the forensic image and I created a virtual machine out of it.

Q. And did you then operate the program?

A. Yes, I powered on the virtual machine.

MR. LOCKARD: If we can turn to page 97?

Q. What is shown here on page 97?

A. This is the main screen that appeared once the DBAN program has booted up.

Q. In the paragraph that is highlighted in red underneath the titled: "Darik's Boot and Nuke About," what is shown there?

A. That is information about the Boot and Nuke program and essentially describes what it is and what it is capable of.

Q. What does it describe, if you could just read that please?

A. Darik's Boot and Nuke (DBAN) is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction.

MR. LOCKARD: And if we can turn to page 98?

Q. Is this an additional screen that is displayed when you operated the Darik's Boot and Nuke program?

A. Yes.

Q. And what does it say in the red box?

A. It says: Warning: This software irrecoverably destroys data.

Q. And down below I think there is a command for listing the quick commands. Did you list the quick commands?

A. I did.

MR. LOCKARD: If we can turn to page 99?

Q. So, generally speaking, what is described in these various commands that are listed in this menu?

A. So these different types of wipes indicate different methods of actually wiping data from a drive. I mentioned before how a standard wipe would write a zero to every available slot on a hard drive. Some organizations and some -- some organizations have developed certain types of wipes that they require or recommend, for instance a three-pass wipe which would be writing a single pass of zeros over the entire drive three times.

Q. Now, in your review of the defendant's computer equipment and electronic accounts, did you find additional evidence relating to data destruction?

A. Yes.

MR. LOCKARD: Ms. Cooper, can we turn to page 102?

THE COURT: Mr. Lockard, does it make sense to stop here for the day or is this a quick --

MR. LOCKARD: This is fine, your Honor.

THE COURT: So then we will break there because it is 2:44.

Ladies and gentlemen, a couple instructions, first the

usual ones. Don't discuss the case. Again, because it is weekend you will likely be seeing family and friends, I hope, but avoid the temptation to talk to them about the case in any way, shape, or form. Don't discuss this with anyone. Don't communicate about it any way, shape, or form. Don't do any research about the case. Keep an open mind.

A couple things and reminders. First, just a reminder that we will not be sitting next Friday but my plan is to sit the four days before then and then we will break for Friday. I know a couple of you had travel over the holiday weekend that you had alerted us to during voir dire. We are going to discuss that probably early next week, see where the case stands, evaluate a variety of things. So bottom line is keep Ms. Smallman apprised of any changes that you have been able to make. Don't incur any greater expense without discussing it with her but just keep her posted where things stand and then we will try to take care of things and address it. Obviously I want to balance keeping the case moving and getting all of you out of here as early as we can without imposing too much on any one of you if you had alerted us to prior commitments.

So the bottom line is more to be discussed on that front next week.

With that, I wish you a very pleasant weekend. We will pick up the same time on Monday, please be here at the same time again and hopefully we will get started promptly at

that time.

Enjoy your weekends. Thank you.

(Continued on next page)

(Jury not present)

THE COURT: You may be seated.

Mr. Berger, you may step down. You are excused for the weekend. Please be here Monday morning no later than 8:45 so that we can get started promptly when we are ready to go.

Have a nice weekend.

THE WITNESS: Thank you.

(Witness steps down)

THE COURT: Mr. Lockard, an estimate of how much longer on direct?

MR. LOCKARD: I would give a rough estimate of about another hour and a half.

THE COURT: And I just skimmed through the demonstrative exhibit. First of all, again, as with 1703, to the extent that you think any of this is admissible under 1006 the burden is on you to extract it and present it. Some of this seems pretty cumulative of areas that were covered through Mr. Leedom. Is it your intention to go through the entirety of this? Am I missing something?

MR. LOCKARD: I think there are some discrete issues in those areas that we do want to hit but I think we are going to move through it pretty quickly and, of course, are conscious of the cumulativeness issue.

THE COURT: I will take it as it comes but I would urge you to pare things down, make sure you are not going over

ground that we have already covered.

Who are the next witnesses coming up the next couple of days?

MR. LOCKARD: So after Mr. Berger concludes we expect to call Jeremy Weber. After Jeremy weber we expect to call Frank Stedman. And then what happens after that depends a little bit on where we are in the week.

THE COURT: OK. Very good.

Mr. Schulte, I would just urge you over the weekend to try to review your anticipated cross. I think some of the cross that you did on Mr. Leedom, I think it got very bogged down into technical details and in that sense, both the trees and the forest may have been lost on the jury. I don't want that to happen again but, more broadly, I don't think it is fair to use the witness as a summary witness just to elicit hearsay and things that they may have heard or other things in the record. If there is stuff in the record that you can argue from, you can argue from it. If it is the kind of thing that the witness would rely on in the course of their expertise and you want to ask how it impacts their analysis that is fair game. But using the witness as a conduit to present hearsay to the jury is not fair game.

The other thing is I think that just as there is case law that says that you can't simply float some hypothetical alternative perpetrator unless there is a nexus to the case and

some evidentiary basis for it. I think so, too, asking questions about some theoretical possibility of some, you know, remote way in which, in theory, someone could have accessed the data here, unless there is some evidence to support it, I don't think that that -- I think that that is sort of the same kind of thing and in that sense, just asking is it theoretically possible that somebody could have accessed it in this way with green men from Mars, that's not fair game. I think if there is evidentiary basis for it that is one thing. If it is just eliciting from a witness that in a theoretical universe some other way of doing this might have happened, that's not OK.

I don't know if the government wishes to add anything on that. I assume you would agree, but.

MR. DENTON: Yes, your Honor. I think we were going to make some observations about it this afternoon. Hopefully, since Mr. Leedom is finished, this is not likely to be an issue to recur.

THE COURT: Well, it is certainly not going to occur on Mr. Leedom but I was just floating it to the extent that it implicates cross for Mr. Berger.

Yes, Mr. Schulte?

MR. SCHULTE: I was just going to say I don't think it is an issue for Mr. Berger. I think some of the issue was simply because there were no logs available that I think some of that was acceptable to raise because they don't know

exactly -- they didn't examine these types of things. But for Berger I don't anticipate anything like that.

THE COURT: Good. Then it is a moot point at this point.

We are going to reconvene in classified setting in short order but before we do that, I want to see if there is anything else to discuss in this setting.

Mr. Denton?

MR. DENTON: Your Honor, we would just ask that the Court again make sort of appropriate findings and allocute the defendant on the record about his control of his own defense.

THE COURT: I really don't think there is any doubt about it but, in any event, no harm in belt and suspenders.

So, Mr. Schulte, is it correct that you continue to control your defense and that you are consulting standby counsel only as needed and on your own volition?

MR. SCHULTE: Yes. That's correct.

THE COURT: Anything that you wish to raise in this setting, Mr. Schulte?

MR. SCHULTE: Yes.

I just want to raise that the government's letter I got very late yesterday in the SCIF and the marshals were kind enough to let me stay until 5:00 but I still wasn't able to, I don't think, really prepare. I don't know if there is any way that I could get an hour in the SCIF or something to be able to

specifically go through the letter and come back with things. That would be helpful.

THE COURT: This is the letter pertaining to the defense witnesses?

MR. SCHULTE: Yes. That's right.

THE COURT: Well, my thought was that we should have a break before we reconvene so in that sense it would permit you some time to do that. It is 2:52. I propose we reconvene at 3:45, which is almost an hour. Obviously you need to be transported to and from the SCIF but does that work?

THE MARSHAL: Yes, sir.

THE COURT: All right. Does that work for the government?

MR. DENTON: Yes, your Honor.

THE COURT: Mr. Schulte?

MR. SCHULTE: Yes. I just want to, on the record, the marshals have been very great in all of this helping facilitate this stuff, so.

THE COURT: Well, I very much appreciate that. I am glad to hear it. Certainly they have been very accommodating to my requests as well and I have told the Marshal himself that I appreciate the deputies here and how good a job they've been doing from my standpoint, but glad to hear it as well.

So if there is nothing further to discuss here, I will give you as much time as we can. Let's plan to reconvene in

the secure setting at 3:45. Obviously, Mr. Schulte, to the extent that we can go through all of the particulars in the government's letter to the extent that the sooner things are resolved the better we can. I guess one question is whether and to what extent you are prepared to respond or would need or want to respond in writing. I think there are some timing issues but I think everybody has an interest in getting some clarity sooner rather than later.

With that, we are adjourned for the day and we will reconvene at 3:45 in the secure setting. I trust that you guys know where it is or you will ask, otherwise trial will reconvene here on Monday morning.

Have a pleasant weekend those of you who will not be in the other courtroom. Thank you.

(Adjourned to June 27, 2022, at 9:00 a.m.)

INDEX OF EXAMINATION

DEFENDANT EXHIBITS